Contemporary Mathematics

Algebraic Geometry Over Four Rings and the Frontier to Tractability

J. Maurice Rojas

This paper is dedicated to Steve Smale on the occasion of his $70^{\underline{\text{th}}}$ *birthday.*

Abstract. We present some new and recent algorithmic results concerning polynomial system solving over various rings. In particular, we present some of the best recent bounds on:

(a) the complexity of calculating the complex dimension of an algebraic set
(b) the height of the zero-dimensional part of an algebraic set over $\mathbb{C}$
(c) the number of connected components of a semi-algebraic set

We also present some results which significantly lower the complexity of deciding the emptiness of hypersurface intersections over $\mathbb{C}$ and $\mathbb{Q}$, given the truth of the Generalized Riemann Hypothesis. Furthermore, we state some recent progress on the decidability of the prefixes $\exists\forall\exists$ and $\exists\exists\forall\exists$, quantified over the positive integers. As an application, we conclude with a result connecting Hilbert's Tenth Problem in three variables and height bounds for integral points on algebraic curves.

This paper is based on three lectures presented at the conference corresponding to this proceedings volume. The titles of the lectures were "Some Speed-Ups in Computational Algebraic Geometry," "Diophantine Problems Nearly in the Polynomial Hierarchy," and "Curves, Surfaces, and the Frontier to Undecidability."

Contents

1. Introduction

This paper presents an assortment of algorithmic and combinatorial results that the author hopes is useful to experts in arithmetic geometry and diophantine complexity. While the selection of results may appear somewhat eclectic, there is an underlying motivation: determining the boundary to tractability for polynomial equation solving in various settings. The notion of tractability here will mean

To appear in a volume of Contemporary Mathematics: Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1–5, 1999), edited by Jan Denef, Leonard Lipschitz, Thanases Pheidas, and Jan Van Geel, AMS Press. This research was partially supported by a Hong Kong CERG Grant.

membership in a particular well-known complexity class depending on the underlying ring and input encoding. As an example of this principle, we point out that our brief tour culminates with a result giving evidence for the following assertion: The recursive unsolvability of deciding the existence of integral roots for multivariate polynomials begins with polynomials in **three** variables. The sharpest current threshold is still nine variables (for **positive** integral roots) [**Jon82**].[1]

Our main results will first be separated into the underlying ring of interest, here either $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, or $\mathbb{Z}$. Within each group of results, we will warm up with a non-trivial result involving univariate polynomials. All necessary proofs are elaborated in section 6, and our main underlying computational models will either be the classical **Turing machine** [**Pap95**] or the **BSS machine over $\mathbb{C}$** [**BCSS98**]. The two aforementioned references are excellent sources for further complexity-theoretic background, but we will only require a minimal acquaintance with these computational models.

Before embarking on the full technical statements of our main theorems, let us see some concrete examples to whet the readers appetite, and further ground the definitions we will later require.

1.1. A Sparse 3×3 Polynomial System.

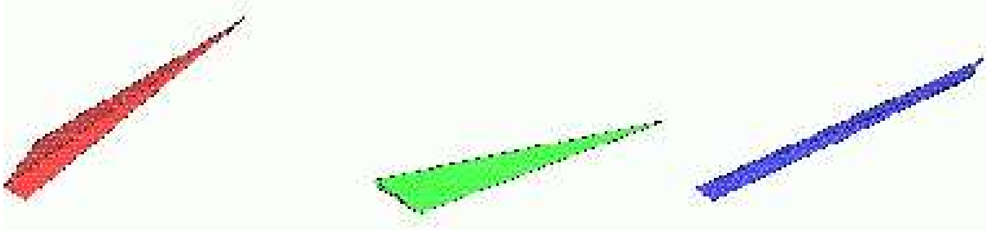
The solution of sparse polynomial systems is a problem with numerous applications outside, as well as inside, mathematics. The analysis of chemical reactions [**GH99**] and the computation of equilibria in game-theoretic models [**MM95**] are but two diverse examples.

More concretely, consider the following system of 3 polynomial equations in 3 variables:

$$\begin{array}{rcl} 144 + 2x - 3y^2 + x^7y^8z^9 & = & 0 \\ -51 + 5x^2 - 27z + x^9y^7z^8 & = & 0 \\ 7 - 6x + 8x^8y^9z^7 - 12x^8y^8z^7 & = & 0. \end{array} \tag{1}$$

Let us see if the system (1) has any **complex** roots and, if so, count how many there are. Any terminology or results applied here will be clarified further in section 2.

Note that the total degree[2] of each polynomial above is 24. By an $18^{\underline{\text{th}}}$-century theorem of Étienne Bézout [**Sha94**], we can bound from above the number of complex roots of (1), assuming this number is finite, by $24 \cdot 24 \cdot 24 = \mathbf{13824}$. However, a more precise $20^{\underline{\text{th}}}$-century bound can be obtained by paying closer attention to the monomial term structure of (1): Considering the convex hull of[3] the exponent vectors of each equation in (1), one obtains three tetrahedra.



[1] James P. Jones, the author of [**Jon82**], attributes the nine variables result to Matiyasevich.

[2] The **total degree** of a polynomial is just the maximum of the sum of the exponents in any monomial term of the polynomial.

[3] i.e., smallest convex set in $\mathbb{R}^3$ containing...

These are the **Newton polytopes** of (1), and their **mixed volume**, by a beautiful theorem of David N. Bernshtein from the 1970's [**Ber75**], turns out to be a much better upper bound on the number of complex roots (assuming there are only finitely many). For our polynomial system (1), this bound is[4] **145**.

Now to decide whether (1) has any complex roots, we can attempt to find a univariate polynomial whose roots are some simple function of the roots of (1). **Elimination theory** allows one to do this, and a particularly effective combinatorial algorithm is given in theorem 2 of section 2. For example, the roots of

$$\begin{gathered}
\boldsymbol{P(u)} := 268435456u^{145} - 138160373760u^{137} - 30953963520u^{130} + 3446308601856u^{129} - 25165824000u^{123} \\
-26293995307008u^{122} - 1694282972921856u^{121} + 323419618934784u^{120} - 6995155353600u^{115} \\
+87379566133248u^{114} + 10198949486395392u^{113} - 16609950177479884 8u^{112} - 112538419200u^{108} \\
-82834929745920u^{107} - 324798104395579392u^{106} - 4419977097552592896u^{105} + 589824000000u^{101} \\
-35724722176000u^{100} + 8364740005330944u^{99} + 4439548695657775104u^{98} - 26917017845238005760u^{97} \\
+37910937600000u^{93} + 51523633570381824u^{92} - 1791672886920019968u^{91} - 84816025002718352 1792u^{90} \\
+61699699935528144 0768u^{89} - 664995358310400u^{85} + 1524560547831644160u^{84} + 74586349797017267 4048u^{83} \\
+1753960334789149 7287680u^{82} + 9942100062141532 07808u^{81} + 12899450880000u^{78} - 4732288823328 7680u^{77} \\
+33981667956844904448u^{76} - 498650298710181363 3024u^{75} + 119063825168001672019968u^{74} \\
+31576057329392164012032u^{73} + 751796121600000u^{70} - 9866721074229006336u^{69} \\
+1882463818496535244800u^{68} + 305287140844065411281 6640u^{67} + 380423482789919103664128u^{66} \\
+348669430145586749767 68u^{65} + 279569449114214400u^{62} - 30217384707872885452 8u^{61} \\
-5347020704648120222 23872u^{60} - 14973258769647086979053568u^{59} + 499421801203658871216 5376u^{58} \\
-2021795433676800u^{55} + 8296585706519424000u^{54} + 25005465159580886376960u^{53} - 37837992627491906773215 36u^{52} \\
+3591638889923283050994 2784u^{51} + 631674139346686588671 5904u^{50} - 61674073526016000u^{47} \\
-5545253022007217448 96u^{46} + 81216323043587727331 9104u^{45} - \underline{29474355965036530602893 76000}u^{44} \\
-14178078125861824498054 3488u^{43} + 6318299549796897024u^{39} - 4109627994682687282 1088u^{38} \\
+29423677023187758191354 0688u^{37} + 32625314371992463523973 0432u^{36} - 8845750586564412369214464u^{35} \\
-29428437386188800u^{32} + 8861566712378831121 60u^{31} - 1203394269299028644809 3392u^{30} \cdots \\
-2134568120341453484944 0320u^{29} + 176061998413186705562222592u^{28} - 8770384173478164480u^{24} \\
+25817804848660579096 3020u^{23} + 48201974945205943116 4020u^{22} - 11741024693522572606851840u^{21} \\
+32803667644608000u^{17} - 3065470746100512257520u^{16} - 4365124819437330950400u^{15} \\
+272459282567626190070720u^{14} + 1910232881488585 4400u^{9} + 12645306845858008350u^{8} \\
-2606594221714946338575u^{7} - 48803823903916800u^{2} + 8681150210659989300
\end{gathered}$$

are exactly those numbers of the form $\alpha\beta\gamma$, where (α, β, γ) ranges over all the roots of (1) in $\mathbb{C}^3$. The above **univariate reduction** thus tells us that our example indeed has finitely many complex roots — exactly[4] 145, in fact. The above polynomial took less than 13 seconds to compute using a naive application of **resultants** and factorization on the computer algebra system `Maple`. Interestingly, computing the same univariate reduction via a naive application of **Gröbner bases** (on the same machine with the same version of `Maple`) takes over 3 hours and 51 minutes.[4]

Admittedly, computing polynomials like the one above can be an unwieldy approach to deciding whether (1) has a complex root. An alternative algorithm, discovered by Pascal Koiran in [**Koi96**] and improved via theorem 4 of section 2 here, makes a remarkable simplification depending on conjectural properties of the distribution of prime ideals in number fields.

For instance, an unoptimized implementation of this alternative algorithm would run as follows on our example:

[4] Please see the Appendix for further details on the theory and implementation behind our examples.

Assumption 1 The truth of the **Generalized**[5] **Riemann Hypothesis (GRH)**.

Assumption 2 Access to an **oracle**[6] which can do the following: Given a finite set of polynomials $F \subset \mathbb{Z}[x,y,z]$ and a finite subset $S \subset \mathbb{N}$, our oracle can decide if there is a prime $p \in S$ such that the mod p reduction of F has a root mod in $\mathbb{Z}/p\mathbb{Z}$.

Step 1 Pick a (uniformly distributed) random integer $t \in \{5\cdot 10^6, \ldots, 5\cdot 10^6 + 2\cdot 10^{11}\}$.

Step 2 Using our oracle, decide if there is a prime $p \in \{2\cdot 10^{22}\cdot t^3, \ldots, 2\cdot 10^{22}\cdot (t+1)^3 - 1\}$ such that the mod p reduction of (1) has a root in $\mathbb{Z}/p\mathbb{Z}$. If so, declare that (1) has a complex root. Otherwise, declare that (1) has no complex root. ■

The choice of the constants above, and the importance of oracle-based algorithms, are detailed further in section 2. In particular, the constants are simply chosen to be large enough to guarantee that, under GRH, the algorithm never fails (resp. fails with probability $\leq \frac{1}{3}$) if (1) has a complex root (resp. does not have a complex root). Thus, for our example, the algorithm above will always give the right answer regardless of the random choice in Step 1. Note also that while the prime we seek above may be quite large, the number of **digits** needed to write any such prime is at most **56** — not much bigger than 53, which is the total number of digits needed to write down the coefficients and exponent vectors of (1). We will explain the complexity-theoretic relevance of this fact in section 2 as well. For the sake of completeness, we observe[4] that the number of real roots of (1) is exactly **11**. While we will not pursue the complexity of real root counting at length in this paper, we will quantitatively explore a more general problem over the reals. Another example follows.

1.2. A Family of Polynomial Inequalities.

In theorem 10 of section 3, we present a new bound on the number of connected components of the solution set of any collection of polynomial inequalities over the real numbers. Bounds of this type have many applications — for example, lower bounds in complexity theory [**DL79, SY82**] and geometric modelling.

As a simple example, let $S_{a,b}(d,n,p,s) \subseteq \mathbb{R}^n$ be the solution set of the following collection of p equalities and s inequalities:

$$\begin{array}{rcll} a_{(\ell,0)} + \left(\sum\limits_{i=1}^{n-1} a_{(\ell,i)} x_i\right) + \sum\limits_{i=1}^{d} b_{(\ell,i)} (x_1 x_2 \cdots x_n)^i & = & 0\ ; & \ell \in \{1,\ldots,p\} \\ (2)\ a_{(p+\ell,0)} + \left(\sum\limits_{i=1}^{n-1} a_{(p+\ell,i)} x_i\right) + \sum\limits_{i=1}^{d} b_{(p+\ell,i)} (x_1 x_2 \cdots x_n)^i & > & 0\ ; & \ell \in \{1,\ldots,s\} \end{array}$$

for any $d,n,p,s \in \mathbb{N}$ and real $a_{(i,j)}$ and $b_{(i,j)}$.

By a bound proved independently by three sets of authors between the 1940's and the 1960's [**OP49, Mil64, Tho65**], we immediately obtain that $S_{a,b}(d,n,p,s)$ has at most $\boldsymbol{(dns+1)(2dns+1)^n}$ connected components.

However, a much sharper bound can be obtained by again looking more closely at the monomial term structure involved: Let Q_F be the convex hull of the union of

[5] The **Riemann Hypothesis (RH)** is an 1859 conjecture equivalent to a sharp quantitative statement on the distribution of primes. GRH can be phrased as a generalization of this statement to prime ideals in an arbitrary number field. Further background on these RH's can be found in [**LO77, BS96**].

[6] i.e., a machine, or powerful being, which can always instaneously and correctly answer such questions. The particular oracle we specify above happens to be an **NP-oracle** [**Pap95**].

the origin $\mathbf{O}$, the standard basis vectors $e_1, \ldots, e_n$ of $\mathbb{R}^n$, and the set of exponent vectors from all the polynomials of (2). (In this case, Q_F happens to be a bipyramid with one apex at $\mathbf{O}$ and the other at $(d, \ldots, d)$.) Normalizing n-dimensional volume, $\mathrm{Vol}_n(\cdot)$, so that the volume of the n-simplex with vertices $\{\mathbf{O}, e_1, \ldots, e_n\}$ is 1, let $V_F := \mathrm{Vol}_n(Q_F)$. Theorem 10 then says that $\min\{n+1, \frac{s+1}{s-1}\}(2s)^n V_F =$ $\boldsymbol{\min\{n+1, \frac{s+1}{s-1}\}(2s)^n(d+1)}$ is also an upper bound on the number of connected components.

We have thus improved the older bound by a factor of over $s(dn)^n$ (modulo a nonzero multiplicative constant), for this family of **semi-algebraic**[7] sets. A broader comparison of our bound to earlier work appears in section 3.1.

Let us now fully state our results over $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$.

2. Computing Complex Dimension Faster

Let $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, $\boldsymbol{F} := (f_1, \ldots, f_m)$, and let $\mathbf{HN}_{\mathbb{C}}$ denote the problem of deciding whether an input F has a complex root.[8] Also let $\mathbf{HN}$ denote the restriction of this problem to polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$. We will respectively consider the complexity of $\mathbf{HN}$ and $\mathbf{HN}_{\mathbb{C}}$ over the Turing-machine model and the BSS model over $\mathbb{C}$.

However, before stating any complexity bounds, let us first clarify our notion of input size: With the Turing model, we will assume that any input polynomial is given as a sum of monomial terms, with all coefficients **and** exponents written in, say, base 2. The corresponding notion of **sparse size** is then simply the total number of bits in all coefficients and exponents. For example, the sparse size of $x_1^D + ax_1^3 + b$ is $\mathcal{O}(\log D + \log a + \log b)$. The sparse size can be extended to the BSS model over $\mathbb{C}$ simply by counting just the total number of bits necessary to write down the exponents (thus ignoring the size of the coefficients).

Note that the number of complex roots of the polynomial $x_1^D - 1$ is already exponential in its sparse size. This behavior is compounded for higher-dimensional polynomial systems, and even affects decision problems as well as enumerative problems. For example, consider the following theorem.

Theorem 1. [**Pla84**] $\mathbf{HN}$ *is* $\mathbf{NP}$*-hard, even in the special case of two polynomial in one variable. More precisely, if one can decide whether an arbitrary input polynomial* $f \in \mathbb{Z}[x_1]$ *of degree* D *vanishes at a* $D^{\underline{\text{th}}}$ *root of unity, within a number of bit operations polynomial in the sparse size of* f*, then* $\mathbf{P} = \mathbf{NP}$. ■

So even for systems such as $f(x_1) = x_1^D - 1 = 0$, $\mathbf{HN}$ may be impossible to solve within bit complexity polynomial in $\log D$ and the sparse size of f. An analogue of this result for $\mathbf{HN}_{\mathbb{C}}$ (theorem 8) appears in the next section.

On the other hand, via the classical Sylvester resultant [**GKZ94**, Ch. 12] and some basic complexity estimates on arithmetic operations [**BCS97**], it is easy to see that this special case of $\mathbf{HN}$ can be decided within a number of bit operations

[7] A **semi-algebraic set** is simply a subset of $\mathbb{R}^n$ defined by the solutions of a finite collection of polynomial inequalities.

[8] We say that F is **feasible** (resp. **infeasible**) over $\mathbb{C}$ iff F has (resp. does not have) a root in $\mathbb{C}^n$.

quadratic in D and the sparse size of f. In complete generality, it is known that $\mathbf{HN} \in \mathbf{PSPACE}$ — an important subclass of **EXPTIME** [**Koi97**].[9]

Alternatively, if one simply counts arithmetic operations (without regard for the size of the intermediate numbers), one can similarly obtain an **arithmetic** complexity upper bound of $\mathcal{O}(D^2)$ for the special case of $\mathbf{HN}_{\mathbb{C}}$ corresponding to the univariate problem mentioned in theorem 1. More generally, it is known that $\mathbf{HN}_{\mathbb{C}}$ is $\mathbf{NP}_{\mathbb{C}}$-complete[10] [**BSS89, Shu93**].

Curiously, efficient **randomization-free** algorithms for **HN** and $\mathbf{HN}_{\mathbb{C}}$ are hard to find in the literature. So we present such an algorithm, with an explicit complexity bound, for a problem including $\mathbf{HN}_{\mathbb{C}}$ as a special case.

THEOREM 2. *Let Z_F be the zero set of F in $\mathbb{C}^n$ and $\dim Z_F$ the complex dimension of Z_F. Also let $\mathbf{O}$ be the origin, and $e_1, \ldots, e_n$ the standard basis vectors, in $\mathbb{R}^n$. Normalize n-dimensional volume $\mathrm{Vol}_n(\cdot)$ so that the volume of the standard n-simplex (with vertices $\mathbf{O}, e_1, \ldots, e_n$) is 1. Finally, let k be the total number of monomial terms in F (counting repetitions between distinct f_i) and let Q_F be the convex hull of the union of $\{\mathbf{O}, e_1, \ldots, e_n\}$ and the set of all exponent vectors of F. Then there is a deterministic[11] algorithm which computes $\dim Z_F$, and thus solves $\mathbf{HN}_{\mathbb{C}}$, within $\mathcal{O}(n^4 k M_F^{2.376} V_F^5 + nk \log(m+n))$ arithmetic operations, where $V_F := \mathrm{Vol}_n(Q_F)$ and M_F is no larger than the maximum number of lattice points in any translate of $(n+1)Q_F$.*

Via a height[12] estimate from theorem 5 later in this section one can also derive a similar bound on the bit complexity of **HN**. We clarify the benefits of our result over earlier bounds in section 2.1. The algorithm for theorem 2, and its correctness proof, are stated in section 6.1. The techniques involved will also be revisited in our discussion of quantifier prefixes over $\mathbb{Z}$ in section 5.

There is, however, a fundamentally different approach which, given the truth of GRH, places **HN** in an even better complexity class. First recall that randomized decision algorithms which answer incorrectly with probability, say, $\leq \frac{1}{3}$, and for which the number of bit operations and random bits needed is always polynomial in the input size, define the complexity class **BPP**.[13] Recall also that when a **BPP** algorithm is augmented by an oracle in **NP**, and the number of oracle-destined bits is always polynomial in the input size, one obtains the class $\mathbf{BPP}^{\mathbf{NP}}$. Finally, when just **one** oracle call is allowed in a $\mathbf{BPP}^{\mathbf{NP}}$ algorithm, one obtains the **Arthur-Merlin class AM** [**Zac86**].

THEOREM 3. [**Koi96**] *Assuming the truth of GRH,* $\mathbf{HN} \in \mathbf{AM}$. ■

[9] While **PSPACE** has important relations to **parallel** algorithms (i.e., algorithms where several operations are executed at once by several processors [**Pap95**]), we will concentrate exclusively on **sequential** (i.e., non-parallel) algorithms in this paper.

[10] This is the analogue of **NP**-complete for the BSS model over $\mathbb{C}$ [**BCSS98**].

[11] i.e., randomization-free

[12] The (absolute multiplicative) **height** of an algebraic number ζ is an important number-theoretic invariant related to the minimal polynomial of ζ over $\mathbb{Z}$. Height bounds are also intimately related to more pedestrian quantities like the maximum absolute value of a coordinate of an isolated root of a polynomial system, so we use the term "height" in this collective sense. Further details on heights, and their extension to $\mathbb{C}^n$, can be found in [**Sil95b, Mal00b, KPS00**].

[13] We emphasize that such algorithms can give different answers when run many times on the same input. However, by accepting the most popular answer of a large sample, the error probability can be made arbitrarily small.

While probabilistic algorithms for **HN** (and more general problems) have certainly existed at least since the early 1980's, the above theorem is the first and only example of an algorithm for **HN** requiring a number of bit operations just **polynomial** in the input size, albeit modulo two strong assumptions.

In view of the vast literature on GRH from both number theory and theoretical computer science, the study of algorithms depending on GRH is not unreasonable. For example, the truth of GRH implies a polynomial-time algorithm for deciding whether an input integer is prime [**Mil76**]. Likewise, in view of the continuing open status of the $\mathbf{P} \overset{?}{=} \mathbf{NP}$ question, oracle-based results are well-accepted within theoretical computer science.[14] In particular, Koiran's conditional result gives the smallest complexity class known to contain **HN**. Indeed, independent of GRH, while it is known that $\mathbf{NP} \subseteq \mathbf{AM} \subseteq \mathbf{PSPACE}$ [**Pap95**], the properness of each inclusion is still an open problem.

The simplest summary of Koiran's algorithm is that it uses reduction modulo specially selected primes to decide feasibility over $\mathbb{C}$. (His algorithm is unique in this respect since all previous algorithms for **HN** worked primarily in the ring $\mathbb{C}[x_1, \ldots, x_n]/\langle F\rangle$.) The key observation behind Koiran's algorithm is that an F infeasible (resp. feasible) over $\mathbb{C}$ will have roots in $\mathbb{Z}/p\mathbb{Z}$ for only finitely many (resp. a positive density of) primes p.

A refined characterization of the difference between positive and zero density can be given in terms of our framework as follows:

THEOREM 4. *Following the notation above, assume now that $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$, let*[15] *$\sigma(F)$ be the maximum of $\log|c|$ as c ranges over the coefficients of all the monomial terms of F, and let D be the maximum total degree of any f_i. Then there exist $a_F, A_F \in \mathbb{N}$, with the following properties:*

(a) *F infeasible over $\mathbb{C} \Longrightarrow$ the reduction of F mod p has a root in $\mathbb{Z}/p\mathbb{Z}$ for at most a_F distinct primes p, and $a_F = \mathcal{O}(n^3 D V_F (4^n D \log D + \sigma(F) + \log m))$.*

(b) *Given the truth of GRH, F feasible over $\mathbb{C} \Longrightarrow$ for each $t \geq 4963041$, the sequence $\{A_F t^3, \ldots, A_F (t+1)^3 - 1\}$ contains a prime p such that the reduction of F mod p has a root in $\mathbb{Z}/p\mathbb{Z}$. Furthermore, we can take $A_F = O\left([V_F \sigma(h_F)(n \log D + \log \sigma(F))]^2\right)$, where h_F is the polynomial defined in theorem 5 below.*

In particular, the bit-sizes of a_F and A_F are both $\mathcal{O}(n \log D + \log \sigma(F))$ — subquadratic in the sparse size of F. Simple explicit formulae for a_F and A_F appear in remarks 12 and 13 of section 6.1.

Via theorem 4, Koiran's algorithm for **HN** can be paraphrased as follows:[16]

Assumption 1 The truth of GRH.
Assumption 2 Access to an **NP**-oracle.
Step 1 Pick a (uniformly distributed) random integer $t \in \{4963041, \ldots, 4963041 + 3a_F\}$.
Step 2 Using our oracle, decide if there is a prime $p \in \{A_F t^3, \ldots, A_F (t+1)^3 - 1\}$ such that F has a root mod p. If so, declare that F has a complex root. Otherwise, declare that F has no complex root. ■

[14] It turns out that $\mathbf{P} = \mathbf{NP}$ also implies the existence of a polynomial-time algorithm for primality testing [**Pra75**].

[15] We point out that in [**Koi96**], the notation $\sigma(F)$ was instead used for a different quantity akin to $2 + mD$.

[16] We point out that, to the best of the author's knowledge, this is the first time that the constants underlying Koiran's algorithm have been made explicit.

In particular, it follows immediately from theorem 4 that the algorithm above is indeed an **AM** algorithm, and that the error probability is $\leq \frac{1}{3}$. Better still, the error probability can be replaced by an arbitrarily small constant ε (keeping the same asymptotic complexity), simply by replacing $3a_F$ by $\frac{1}{\varepsilon}a_F$ in Step 1 above.

The proof of theorem 4 is based in part on a particularly effective form of univariate reduction.

Theorem 5. *Following the notation above, and the assumptions of theorem 4, there exist a univariate polynomial $h_F \in \mathbb{Z}[u_0]$ and a point $u_F := (u_1, \ldots, u_n) \in \mathbb{Z}^n$ with the following properties:*

0. *The degree of h_F is $\leq V_F$.*
1. *For any irreducible component W of Z_F, there is a point $(\zeta_1, \ldots, \zeta_n) \in W$ such that $u_1\zeta_1 + \cdots + u_n\zeta_n$ is a root of h_F. Conversely, if $m \leq n$, all roots of h_F arise this way.*
2. *F has only finitely many complex roots $\Longrightarrow$ the splitting field of h_F over $\mathbb{Q}$ is exactly the field $\mathbb{Q}[x_i \mid (x_1, \ldots, x_n) \in \mathbb{C}^n$ is a root of $F]$.*
3. *The coefficients of h_F satisfy $\sigma(h_F) = \mathcal{O}\left(M_F[\sigma(F) + m(n \log D + \log m)] + n^2 V_F \log D\right)$ and, when $m \leq n$, $\sigma(h_F) = \mathcal{O}(M_F \sigma(F) + n^2 V_F \log D)$.*
4. *$m \leq n \Longrightarrow$ the deterministic arithmetic complexity of computing u_F, and all the coefficients of h_F, is $\mathcal{O}(n^3 M_F^{2.376} V_F^5)$.*
5. *We have $\log(1 + |u_i|) = \mathcal{O}(n^2 \log D)$ for all i.*

Note that we have thus obtained the existence of points of bounded height on the positive-dimensional part of Z_F, as well as a bound on the height of any point in the zero-dimensional part of Z_F. Put more simply, via a slight variation of the proof of theorem 5, we obtain the following useful bound:

Theorem 6. *Following the notation of theorem 5, any irreducible component W of Z_F contains a point $(x_1, \ldots, x_n)$ such that for all i, either $x_i = 0$ or $|\log |x_i|| = \mathcal{O}(M_F[\sigma(F) + m(n \log D + \log m)])$. Furthermore, when $m \leq n$, the last upper bound can be improved to $\mathcal{O}(M_F \sigma(F))$.* ■

Our final result over $\mathbb{C}$ is a refinement of theorem 5 which will help simplify the proofs of our results in section 5 on integral points.

Theorem 7. [**Roj99c**] *Following the notation of theorem 5, one can pick u_F and h_F (still satisfying (0)–(5)) so that there exist $a_1, \ldots, a_n \in \mathbb{N}$ and $h_1, \ldots, h_n \in \mathbb{Z}[u_0]$ with the following properties:*

6. *The degrees of $h_1, \ldots, h_n$ are all bounded above by V_F.*
7. *For any root $\theta = u_1\zeta_1 + \cdots + u_n\zeta_n$ of h_F, $\frac{h_i(\theta)}{a_i} = \zeta_i$ for all i.*
8. *For all i, both $\log a_i$ and $\sigma(h_i)$ are bounded above by $\mathcal{O}(V_F^2 \sigma(h_F))$.*
9. *$m \leq n \Longrightarrow$ the deterministic arithmetic complexity of computing all the coefficients of $h_1, \ldots, h_n$ is $\mathcal{O}(n^4 M_F^{2.376} V_F^5)$.*

Explicit formulae for all these asymptotic estimates, as well as their proofs, appear in remarks 9, 10, and 11 of section 6.1. However, let us first compare these quantitative results to earlier work.

2.1. Related Results Over $\mathbb{C}$.

Solving $\mathbf{HN}_{\mathbb{C}}$ too quickly also leads to unexpected collapses of complexity classes as follows.

Theorem 8. *Suppose there is an algorithm (on a BSS machine over $\mathbb{C}$) which decides whether an arbitrary input polynomial $f \in \mathbb{C}[x_1]$ of degree D vanishes at* *a $D^{\underline{\text{th}}}$ root of unity, within a number of arithmetic operations polynomial in the sparse size of f. Then* $\mathbf{NP} \subseteq \mathbf{BPP}$*.* ■

This result is originally due to Steve Smale and a proof appears in [**Roj00b**]. It is currently believed that the inclusion $\mathbf{NP} \subseteq \mathbf{BPP}$ is quite unlikely.

Curiously, finding (as opposed to deciding the existence of) roots for even a seemingly innocent univariate polynomial can lead to undecidability in the BSS model over $\mathbb{C}$:

THEOREM 9. *Determining whether an* **arbitrary** $x_0 \in \mathbb{C}$ *converges to a root of* $x^3 - 2x + 2 = 0$ *under Newton's method is undecidable, relative to the BSS model over* $\mathbb{C}$*.* ■

This result follows easily via a dynamics result of Barna [**Bar56**] and the proof appears in [**BCSS98**, Sec. 2.4]. One should of course note that this result in no way prevents one from finding **some** x_0 which converges to a root of $x^3 - 2x + 2$. So this result is a more a reflection of the subtlety of dynamics than the limits of the BSS model.

As for the other results of section 2, we point out that we have tried to balance generality, sharpness, and ease of proof in our bounds. In particular, our bounds fill a lacuna in the literature where earlier bounds seemed to sacrifice generality for sharpness, or vice-versa.

To clarify this trade-off, first note that $\mathcal{I}_F \leq V_F \leq D^n$, where $\mathcal{I}_F$ is the number of irreducible components of Z_F. (The first inequality follows immediately from theorem 5, while the second follows from the observation that Q_F always lies in a copy of the standard n-simplex scaled by a factor of D.) So depending on the shape of Q_F, and thus somewhat on the sparsity of F, one can typically expect V_F to be much smaller than D^n. For example, our 3×3 system from section 1.1 gives $D^n = 13824$ and $V_F = 243$. Setting $p = n$ and $s = 0$ in the example from section 1.2, it is easy to see that the factor of improvement can even reach D^{n-1}, if not more.

As for the quantities k and M_F, we will see in lemma 1 of section 6.1.1 that $k \leq m(V_F + n)$ and $M_F \leq \binom{nD+1}{n} = \mathcal{O}(e^n(nD+1)^n)$. Furthermore, just as V_F is a much more desirable complexity measure than D^n, we point out that the preceding bound on M_F is frequently overly pessimistic: for example, $M_F = \mathcal{O}(V_F)$ for fixed n. The true definition of M_F appears in section 6.1.1.

Our algorithm for computing $\dim Z_F$ thus gives the first deterministic complexity bound which is polynomial in V_F and M_F. In particular, while harder problems were already known to admit **PSPACE** complexity bounds, the corresponding complexity bounds were either polynomial (or worse) in D^n, or stated in terms of a non-uniform computational model.[17] Our algorithm for the computation of $\dim Z_F$ thus gives a significant speed-up over earlier work.

For example, via the work of Chistov and Grigoriev from the early 1980's on quantifier elimination over $\mathbb{C}$ [**CG84**], it is not hard to derive a deterministic arithmetic complexity bound of $\mathcal{O}((mD)^{n^4})$ for the computation of $\dim Z$. More recently, [**GH93**] gave a randomized arithmetic complexity bound of $m^{\mathcal{O}(1)} D^{\mathcal{O}(n)}$. Theorem 2 thus clearly improves the former bound. Comparison with the latter

[17] For example, some algorithms in the literature are stated in terms of **arithmetic networks**, where the construction of the underlying network is not included in the complexity estimate.

bound is a bit more difficult since the exponential constants and derandomization complexity are not explicit in [**GH93**].

As for faster algorithms, one can seek complexity bounds which are polynomial in even smaller quantities. For example, if one has an irreducible algebraic variety $V \subseteq \mathbb{C}^n$ of complex dimension d, one can define its **affine geometric degree**, $\delta(V)$, to be the number of points in $V \cap H$ where H is a generic $(n-d)$-flat.[18] More generally, we can define $\delta(Z_F)$ to be the sum of $\delta(V)$ as V ranges over all irreducible components of Z_F. It then follows (from theorem 2 and a consideration of intersection multiplicities) that $\mathcal{I}_F \leq \delta(Z_F) \leq V_F$. Similarly, one can attempt to use mixed volumes of several polytopes (instead of a single polytope volume) to lower our bounds.

We have avoided refinements of this nature for the sake of simplicity. Another reason it is convenient to have bounds in terms of V_F is that the computation of $\delta(Z_F)$ is even more subtle than the computation of polytopal n-volume. For example, when n is fixed, $\mathrm{Vol}_n(Q)$ can be computed in polynomial time simply by triangulating the polytope Q and adding together the volumes of the resulting n-simplices [**GK94**]. However, merely deciding $\delta(Z_F) > 0$ is already **NP**-hard for $(m,n) = (2,1)$, via theorem 1. As for varying n, computing $\delta(Z_F)$ is #**P**-hard, while the computation of polytope volumes is #**P**-complete.[19] (The latter result is covered in [**GK94, KLS97**], while the former result follows immediately from the fact that the computation of $\delta(Z_F)$ includes the computation of V_F as a special case.) More practically, for any fixed $\varepsilon_1, \varepsilon_2 > 0$, there is an algorithm which runs in time polynomial in the sparse encoding of F (and thus polynomial in n) which produces a random variable that is within a factor of $1-\varepsilon_1$ of $\mathrm{Vol}_n(Q_F)$ with probability $1-\varepsilon_2$ [**KLS97**]. The analogous result for mixed volume is known only for certain families of polytopes [**GS00**], and the existence of such a result for $\delta(Z_F)$ is still an open problem.

In any event, we point out that improvements in terms of $\delta(Z_F)$ for our bounds are possible, and these will be pursued in a forthcoming paper. Similarly, the exponents in our complexity bounds can be considerably lowered if randomization is allowed. Furthermore, Lecerf has recently announced a randomized arithmetic complexity bound for computing $\dim Z_F$ which is polynomial in $\max_i\{\delta(Z_{(f_1,\ldots,f_i)})\}$ [**Lec00**].[20] However, the complexity of derandomizing Lecerf's algorithm is not yet clear.

As for our result on prime densities (theorem 4), part (a) presents the best current bound polynomial in V_F and M_F. An earlier density bound, polynomial in $D^{n^{\mathcal{O}(1)}}$ instead, appeared in [**Koi96**].

Part (b) of theorem 4 appears to be new, and makes explicit an allusion of Koiran in [**Koi96**].

Remark 1. *We point out that we cheated slightly in our refinement of Koiran's algorithm: We did not take the complexity of computing V_F into account. (It is easy to see that this is what dominates the randomized bit complexity of the algorithm.) This can be corrected, and perhaps the simplest way is to replace every occurence*

[18] We explain the term "generic" in sections 5 and 6.2.3.

[19] #**P** is the analogue of **NP** for enumerative problems (as opposed to decision problems) [**Pap95**].

[20] The paper [**Lec00**] actually solves the harder problem of computing an algebraic description of a non-empty set of points in every irreducible component of Z_F, and distinguishing which component each set belongs to.

of V_F with D^n in our bounds for M_F, a_F, and A_F. Alternatively, if one want to preserve polynomiality in V_F, one can instead apply the polynomial-time randomized approximation techniques of [**KLS97**] *to V_F, and make a minor adjustment to the error probabilities.* ■

Remark 2. *Pascal Koiran has also given an* **AM** *algorithm (again depending on GRH) for deciding whether the complex dimension of an algebraic set is less than some input constant* [**Koi97**]. ■

Regarding our height bound, the only other results stated in polytopal terms are an earlier version of theorem 5 announced in [**Roj99b**], and independently discovered bounds in [**KPS00**, Prop. 2.11] and [**Mai00**, Cor. 8.2.3]. The bound from [**KPS00**] applies to a slightly different problem, but implies (by intersecting with a generic linear subspace with reasonably bounded coefficients)[21] a bound of $\mathcal{O}((4^n D\log n + n\sigma(F))V_F)$ for our setting. Furthermore, by examining a key ingredient in their proof (Proposition 1.7 from [**KPS00**]), their bound can actually be improved to $\mathcal{O}(DM_F \log n + nV_F\sigma(F))$. The last bound is thus close to ours, and can be better when m and $\sigma(F)$ are large and n is small. The bound from [**Mai00**, Cor. 8.2.3] uses Arakelov intersection theory, holds only for $m=n$, and the statement is more intricate (involving a sum of several mixed volumes). So it is not yet clear when [**Mai00**, Cor. 8.2.3] is better than theorem 5. In any case, our result has a considerably simpler proof than either of these two alternative bounds: We use only resultants and elementary linear algebra and factoring estimates.

We also point out that the only earlier bounds which may be competitive with theorems 5 and 6, [**KPS00**, Prop. 2.11], and [**Mai00**, Cor. 8.2.3] are polynomial in $e^n(nD+1)^n$ and make various non-degeneracy hypothesis, e.g., $m=n$ and no singularities for Z_F (see [**Can87**] and [**Mal00a**, Thm. 5]). As for bounds with greater generality, the results of [**FGM90**] imply a height bound for general quantifier elimination which, unfortunately, has a factor of the form $2^{(n\log D)^{\mathcal{O}(r)}}$ where r is the number of quantifier alternations [**Koi96**].

As for theorem 7, the approach of rational univariate representations (**RUR**) for the roots of polynomial systems dates back to Kronecker. RUR also goes under the name of "effective primitive element theorem" and important precursors to theorem 7, with respective complexity bounds polynomial in $e^n(nD+1)^n$ and $D^{n^{\mathcal{O}(1)}}$, are stated in [**Can88**] and [**Koi96**, Thm. 4]. Nevertheless, the use of **toric resultants** (cf. section 6.1), which form the core of our algorithms here, was not studied in the context of RUR until the late 1990's (see, e.g., [**Roj99c**]). In particular, theorem 7 appears to be the first statement giving bounds on $\sigma(h_i)$ which are polynomial in V_F. As for computing $h, h_1, \ldots, h_n$ faster, an algorithm for RUR with randomized complexity polynomial in $\max_i\{\delta(Z_{(f_1,\ldots,f_i)})\}$ was derived in [**GLS99**]. However, their algorithm makes various nondegeneracy assumptions (such as $m=n$ and that F form a complete intersection) and the derandomization complexity is not stated.

The remaining bottle-neck in improving our complexity and height bounds stems from the exponentiality in n present in the quantity M_F. However, the resulting exponential factor, which is currently known to be at worst $\mathcal{O}(e^n)$ (cf. lemma 1 of section 6.1.1), can be reduced to $\mathcal{O}(n)$ in certain cases. In general, this can be done whenever there exists an expression for a particular toric resultant (cf.

[21] Martin Sombra pointed this out in an e-mail to the author.

section 6.1) as a single determinant, or the divisor of a determinant, of a matrix of size $\mathcal{O}(nV_F)$. The existence of such formulae has been proven in various cases, e.g., when all the Newton polytopes are axis-parallel parallelepipeds [**WZ94**]. Also, such formulae have been observed (and constructed) experimentally in various additional cases of practical interest [**EC93**]. Finding compact formulae for resultants is an area of active research which thus has deep implications for the complexity of algebraic geometry.

Finally, we note that we have avoided Gröbner basis techniques because there are currently no known complexity or height bounds polynomial in V_F (or even M_F) using Gröbner bases for the problems we consider. A further complication is that there are examples of ideals, generated by polynomials of degree ≤ 5 in $\mathcal{O}(n)$ variables, where every Gröbner basis has a generator of degree 2^{2^n} [**MM82**]. This is one obstruction to deriving sharp explicit complexity bounds via a naive application of Gröbner bases. Nevertheless, we point out that Gröbner bases are well-suited for other difficult algebraic problems, and their complexity is also an area of active research.

3. Polytope Volumes and Counting Pieces of Semi-Algebraic Sets

Continuing our theme of measuring algebraic-geometric complexity in combinatorial terms, we will see how to bound the number of connected components of a semi-algebraic set in terms of polytope volumes. However, let us first see an unusual example of how input encoding influences computational complexity, as well as geometric complexity, over the real numbers.

Recall that a **straight-line program (SLP)** presents a polynomial as a sequence of subtractions and multiplications, starting from a small set of constants and variables [**BCS97, BCSS98**]. (Usually, the only constant given a priori is 1.) The **SLP size** of a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is then just the minimum of the total number of operations needed by any SLP evaluating to f. Thus, while $(x+2^{2^2})^{1000} - 2^{2^{2^3}}$ has a large sparse size, its SLP size is easily seen to be quite small, via standard recursive tricks such as repeated squaring. SLP's are thus a more powerful encoding than the sparse encoding, since the SLP size of a polynomial is trivially bounded from above by a linear function of its sparse size.

Consider the following corollary of theorem 1.

Corollary 1. *If one can decide whether an arbitrary $f \in \mathbb{Z}[x_1]$ has a real root, within a number of bit operations polynomial in the SLP size of f, then* $\mathbf{P} = \mathbf{NP}$. ■

Thus the hardness of feasibility testing we've observed earlier over $\mathbb{C}$ persists over $\mathbb{R}$, albeit relative to a smaller complexity measure. Peter Bürgisser observed the following simple proof of this corollary in 1998: Assuming the hypothesis above, consider the polynomial system $G := (f(w), w(z+i) - iz)$. Then f has a real root $\Longleftrightarrow G$ has a root (w, z) with w on the unit circle, and our assumption thus implies the existence of a polynomial-time algorithm (relative now to the SLP encoding) for detecting whether certain systems of two polynomials in two variables have a root (w, z) with w on the unit circle. This in turn implies an algorithm, requiring a number of bit operations just polynomial in the sparse size of f, for deciding if a univariate polynomial f has a root on the unit circle. This is not quite the same problem as the special case of **HN** from theorem 1, but it is nevertheless known to be **NP**-hard as well [**Pla84**]. So we finally obtain $\mathbf{P}=\mathbf{NP}$ from our initial assumption and our corollary is thus proved.

Another complication with detecting the existence of real roots too quickly is that the number of real roots, even for a single univariate polynomial, can be exponential in the SLP size. (This fact is **not** implied by our earlier example of x_1^D-1.) To see why, simply consider the recursion $g_{j+1}:=4g_j(1-g_j)$ with $g_1:=4x(1-x)$. It is then easily checked[22] that $g_j(x)-x$ has 2^j roots in the open interval $(0,1)$, but an SLP size of just $\mathcal{O}(j)$.

It is an open question whether corollary 1 holds relative to **sparse** size. More to the point, the influence of sparse size on the number of **real** roots of polynomial systems remains a deep open question. For instance, the classical **Descartes rule of signs** states that any univariate polynomial with real coefficients and k monomial terms has at most $2k+1$ real roots. However, the best known bounds on the number of isolated real roots for 2 polynomials in 2 unknowns are already exponential in the number of monomial terms, even if one restricts to roots with all coordinates positive (cf. section 3.1).

However, one can at least give bounds which are linear in a suitable polytope volume, which apply even in the the more general context of polynomial inequalities.

THEOREM 10. [**Roj00b**] *Let $f_1,\ldots,f_{p+s}\in\mathbb{R}[x_1,\ldots,x_n]$ and suppose $S\subseteq\mathbb{R}^n$ is the solution set of the following collection of polynomial inequalities:*

$$\begin{aligned} f_i(x) &= 0, \quad i\in\{1,\ldots,p\}\\ f_{p+i}(x) &> 0, \quad i\in\{1,\ldots,s\}\end{aligned}$$

Let $Q_F\subset\mathbb{R}^n$ be the convex hull of the union of $\{\mathbf{O},\hat{e}_1,\ldots,\hat{e}_n\}$ and the set of all a with $x^a:=x_1^{a_1}\cdots x_n^{a_n}$ a monomial term of some f_i. Then S has at most

$$\min\{n+1,\frac{s+1}{s-1}\}2^n s^n V_F \text{ (for } s>0) \quad\text{or}\quad 2^{n-1}V_F \text{ (for } s=0)$$

connected components, where $V_F:=\mathrm{Vol}_n(Q_F)$. ■

In closing this brief excursion into semi-algebraic geometry, we point out that unlike the complex case, it is not yet known whether V_F is an upper bound on the number of **real** connected components. This is because a complex component may contribute two or more real connected components. Nevertheless, it is quite possible that the factors exponential in n in our bounds may be removed from our bounds in the near future.

3.1. Related Results Over $\mathbb{R}$.

We first recall the following important result relating sparse size and real roots for certain non-degenerate polynomial systems. (Recall also that the **positive orthant** of $\mathbb{R}^n$ is the subset $\{(x_1,\ldots,x_n)\mid x_i>0 \; for\ all\ i\}$.)

KHOVANSKI'S THEOREM ON REAL FEWNOMIALS. **(Special Case)**[23] [**Kho91**, Sec. 3.12, Cor. 6] *Following the notation of theorem 10, suppose $p=n$, $s=0$, and the Jacobian matrix of F is invertible at any complex root of F. Also let k' be the number of exponent vectors which appear in at least one of $f_1,\ldots,f_n$. Then F has at most $(n+1)^{k'}2^{k'(k'-1)/2}$ real roots in the positive orthant.* ■

[22] This example is well-known in dynamical systems, and the author thanks Gregorio Malajovich for pointing it out.

[23] Khovanski's Theorem on Fewnomials actually holds for a more general class of functions — the so-called **Pfaffian** functions [**Kho91**].

For example, Khovanski's bound readily implies that our 3×3 example from section 1.1 has at most $8\cdot 4^9\cdot 2^{36}=\mathbf{144115188075855872}$ real roots — quite a bit more than 972 (the estimate from theorem 10 above) or 11 (the true number of real roots). Nevertheless, we emphasize that his theorem was a major advance, giving the first bound on the number of real roots independent of the degree of the input polynomials.

As for other more general results, Khovanski also gave bounds on the **Betti numbers**[24] of non-degenerate real algebraic varieties [**Kho91**, Sec. 3.14, Cor. 5]. Similarly, these results (which thus require $p\leq n$ and $s=0$) become more practical as the polynomial degrees grows and the number of monomial terms remains small.

Closer to our approach, Benedetti, Loeser, and Risler independently derived a polytopal upper bound on the number connected components of a real algebraic variety in [**BLR91**, Prop. 3.6]. Their result, while applying only in the case where $p\leq n$ and $s=0$, can give a better bound when the number of equations p is a small constant and n is large. We also point out that their result has a more complicated statement than ours, involving a recursion in terms of mixed volumes of projections of polytopes.

The only other known bounds on the number of connected components appear to be linear in D^n. For example, a bound derived by Oleinik, Petrovsky, Milnor, and Thom before the mid-1960's [**OP49, Mil64, Tho65**] gives $D(2D-1)^{n-1}$ for $s=0$ and $(sD+1)(2sD+1)^n$ for $s>0$. An improvement, also polynomial in D^n, was given recently by Basu [**Bas96**]: $(p+s)^n\mathcal{O}(D)^n$, where the implied constant is not stated explicitly. For $s>0$ our bound is no worse than $\min\{n+1,\frac{s+1}{s-1}\}(2sD)^n$ — better than both preceding bounds and frequently much better. For $s=0$ our bound is no worse than $2^{n-1}D^n$ — negligibly worse than the oldest bound, but asymptotically better than Basu's bound.

For the sake of brevity, we have mainly focused on one combinatorial aspect of semi-algebraic sets. So let us at least mention a few additional complexity-theoretic references: Foundational results on the complexity of solving (or counting the roots of) polynomial systems over $\mathbb{R}$ can be found in [**Roy96**], and faster recent algorithms can be found in [**Roj98, MP98**]. More generally, there are algorithms known for quantifier elimination over any real closed field [**Ren92, Can93, BPR96**].

Curiously, the best current complexity bounds for the problems over $\mathbb{R}$ just mentioned are essentially the same as those for the corresponding problems over $\mathbb{C}$. Notable recent exceptions include [**BGHM97**] and [**RY00**] where the complexity bounds depending mainly on quantities relating only to the underlying real geometry. (The first paper deals with finding a point in every connected component of a semi-algebraic set, while the second paper deals with approximating the real roots of a trinomial within time quadratic in $\log D$.) Also, with the exception of [**BGHM97, Roj98, MP98, RY00**], all the preceding references present complexity bounds depending on n and D^n, with no mention of sharper quantities like V_F.

[24] These are more subtle cohomological invariants which include the number of connected components as a special case (see, e.g., [**Mun84**] for further details).

An interesting question which remains is whether feasibility over $\mathbb{R}$ can be decided within the **polynomial hierarchy** (a collection of complexity classes suspected to lie below **PSPACE** [**Pap95**]), with or without GRH. As we will see now, this can be done over $\mathbb{Q}$ (at least in a restricted sense) as well as $\mathbb{C}$.

4. The Generalized Riemann Hypothesis and Detecting Rational Points

Here we will return to considering computational complexity estimates: We show that deciding feasibility over $\mathbb{Q}$, for most polynomial systems, lies within the polynomial hierarchy, assuming GRH. To fix ideas, let us begin with the case of a single univariate polynomial.

THEOREM 11. [**Len98**] *Suppose $f \in \mathbb{Z}[x_1]$ and $\pm\frac{p}{q} \in \mathbb{Q}$ is a root of f, with $p, q \in \mathbb{N}$ and $\gcd(p,q)=1$. Then $\log p$, $\log q$, and the number of rational roots are all polynomial in $\mathrm{size}(f)$ (the sparse size of f). Furthermore,* **all** *rational roots of f can be computed within $\mathcal{O}(\mathrm{size}(f)^{10})$ bit operations.*[25] ■

Note that the complexity bound above does **not** follow directly from the famous polynomial-time factoring algorithm of Lenstra, Lenstra, and Lovasz [**LLL82**]: their result has complexity polynomial in the degree of f, as well as $\mathrm{size}(f)$. Also, Lenstra actually derived a more general version of the theorem above which applies to finding all bounded degree factors of a univariate polynomial over any fixed algebraic number field [**Len98**]. Interestingly, the analogue of theorem 11 for the **SLP size** is an open problem and, like theorem 1 and corollary 1, has considerable impact within complexity theory (see theorem 15 of section 5 for the full statement).

Curiously, there is currently no known analogue of theorem 11 for **systems** of multivariate polynomials. The main reason is that the most naive generalizations easily lead to various obstructions and even some unsolved problems in number theory. For example, as of mid-2000, it is still unknown whether deciding the existence of a rational root for $y^2 = ax^3 + bx + c$ is even Turing-decidable. Thus, the first obvious restriction to make, following the notation of the last two sections, is to consider only those F where Z_F is finite. But even then there are complications:

- $\mathbf{Q_1}$ The number of integral roots of F can actually be exponential in the sparse size of F: A simple example is the system $(\prod_{i=1}^{D}(x_1 - i), \ldots, \prod_{i=1}^{D}(x_n - i))$, which has D^n integral roots and a sparse size of $\mathcal{O}(nD \log D)$. ■
- $\mathbf{Q_2}$ For $n > 1$, the integral roots of F can have coordinates with bit-length exponential in $\mathrm{size}(F)$, thus ruling out one possible source **NP** certificates: For example, the system $(x_1 - 2, x_2 - x_1^2, \ldots, x_n - x_{n-1}^2)$ has sparse size $\mathcal{O}(n)$ but has $(1, 2, \ldots, 2^{2^{n-2}})$ as a root. ■

So it appears that restricting to deciding the existence of rational roots, instead of finding them, may be necessary for sub-exponential complexity. Nevertheless, these difficulties may disappear when n is fixed: even the case $n=2$ is open.

As for simple complexity upper bounds, the efficient deterministic algorithms of section 2 can easily be converted to **PSPACE** algorithms for finding all rational points within the zero-dimensional part of an algebraic set. However, we will use a different approach to place this problem within an even lower complexity class: testing the densities of primes with certain properties.

[25] The exponent was not stated explicitly in [**Len98**] but, via [**LLL82**], can easily be derived from the description of the algorithm given there.

First note that averaging over many primes (as opposed to employing a single sufficiently large prime) is essentially unavoidable if one wants to use mod p root counts to decide the existence of rational roots. For example, from basic quadratic residue theory [**HW79**], we know that the number of roots x_1^2+1 mod p is **not** constant for sufficiently large prime p. Similarly, Galois-theoretic considerations are also necessary before using mod p root counts to decide feasibility over $\mathbb{Q}$.

EXAMPLE 3. *Take $m=n=1$ and $F=f_1=(x_1^2-2)(x_1^2-7)(x_1^2-14)$. Clearly, F has no rational roots. However, it is easily checked via the Jacobi symbol* [**HW79, BS96**] *that F has a root mod p for* **all** *primes p. In particular, note that the Galois group here is not transitive: there is no automorphism of $\overline{\mathbb{Q}}$ which fixes $\mathbb{Q}$ and sends, say, $\sqrt{2}$ to $\sqrt{7}$.*

So let us now state a precursor to our method for detecting rational roots: Recall that $\pi(x)$ denotes the number of primes $\leq x$. Let $\pi_F(x)$ be the variation on $\pi(x)$ where we instead count the number of primes $p \leq x$ such that the reduction of F mod p has a root in $\mathbb{Z}/p\mathbb{Z}$, and let # denote set cardinality.

THEOREM 12. *(See* [**Roj00c**, Thm. 2]*.) Following the notation of sections 2 and 3, assume now that the coefficients of F are integers. Let K be the field $\mathbb{Q}(x_i \mid (x_1,\ldots,x_n)\in Z_F\ ,\ i\in\{1,\ldots,n\})$. Then the truth of GRH implies the two statements for all $x>33766$:*

1. *Suppose $\infty>\#Z_F\geq 2$ and* $\mathrm{Gal}(K/\mathbb{Q})$ *acts transitively on Z_F. Then*

$$\frac{\pi_F(x)}{\pi(x)} < \left(1-\frac{1}{V_F}\right)\left(1+\frac{(V_F!+1)\log^2 x + V_F!V_F\mathcal{O}(V_F+\sigma(h_F))\log x}{\sqrt{x}}\right).$$

2. *Suppose $\#Z_F\geq 1$. Then independent of* $\mathrm{Gal}(K/\mathbb{Q})$*, we have*

$$\frac{\pi_F(x)}{\pi(x)} > \frac{1}{V_F}(1-b(F,x)),$$

where $0\leq b(F,x)<\frac{4V_F\log^2 x+V_F^2\mathcal{O}(V_F+\sigma(h_F)+nV_F\sigma(h_F)/\sqrt{x})\log x}{\sqrt{x}}$ and $0\leq\sigma(h_F)=$ $\mathcal{O}\left(M_F[\sigma(F)+m(n\log D+\log m)]+n^2V_F\log D\right)$. Better still, we have $\sigma(h_F)=$ $\mathcal{O}(M_F\sigma(F)+n^2V_F\log D)$ when $m\leq n$. ■

The upper bound from assertion (1) appears to be new, and the lower bound from assertion (2) significantly improves earlier bounds appearing in [**Koi96, Mor97, Bür00**] which were polynomial in D^n. Explicit formulae for the above asymptotic estimates appear in [**Roj00c**, Remarks 9 and 10].

Theorem 12 thus presents the first main difference between feasibility testing over $\mathbb{C}$ and $\mathbb{Q}$: from theorem 4, we know that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z}$ for a density of primes p which is either positive or zero, according as F has a root in $\mathbb{C}$ or not. The corresponding gap between densities happened to be large enough for Koiran's randomized oracle algorithm to decide feasibility over $\mathbb{C}$ (cf. section 2). (We point out that Koiran's algorithm actually relies on the behavior of the function N_F defined below, which is more amenable than that of π_F.) On the other hand, assertion (1) of theorem 12 tells us that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z}$ for a density of primes which is either 1 or $1-\frac{1}{V_F}$, according as F has, or **strongly** fails to have, a rational root.

Unfortunately, the convergence of $\frac{\pi_F(x)}{\pi(x)}$ to its limit is unfortunately too slow to permit any obvious algorithm using subexponential work. However, via a Galois-theoretic trick (cf. theorem 14 below) we can nevertheless place rational root detection in a lower complexity class than previously known.

THEOREM 13. [**Roj00c**] *Following the notation and assumptions of theorem 12, assume further that F fails to have a rational root $\Longleftrightarrow$ $[Z_F=\emptyset$ or $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $Z_F]$. Then the truth of GRH implies that deciding whether F has a rational root can be done in polynomial-time, given access to an oracle in $\mathbf{NP}^{\mathbf{NP}}$, i.e., within the complexity class $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$. Also, we can check the emptiness and finiteness of Z_F unconditionally (resp. assuming GRH) within* **PSPACE** *(resp.* **AM***).* ■

The new oracle can be summarized as follows: Given any F and a finite subset $S\subset\mathbb{N}$, our oracle instantaneously tells us whether or not there is a prime $p\in S$ such that the mod p reduction of F has **no** roots in $\mathbb{Z}/p\mathbb{Z}$.

Part of the importance of oracle-based algorithms, such as the one above or the algorithm from section 2, is that it could happen that $\mathbf{P}\neq\mathbf{NP}$ but the higher complexity classes we have been alluding to all collapse to the same level. For example, while it is known that $\mathbf{NP}\cup\mathbf{BPP}\subseteq\mathbf{AM}\subseteq\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}\subseteq\mathbf{NP}^{\mathbf{NP}^{\mathbf{NP}}}\subseteq\cdots\subseteq\mathbf{PSPACE}$, the properness of each inclusion is still unknown [**Zac86, BM88, BF91, Pap95**].

The algorithm for theorem 13 is almost as simple as the algorithm for theorem 4 given earlier, and can be outlined as follows:

Step 0 Let $N_F(x)$ denote the **weighted** version of $\pi_F(x)$ where we instead sum the total number of roots in $\mathbb{Z}/p\mathbb{Z}$ of the mod p reductions of F over **all** primes $p\leq x$.

Step 1 Let t_0^* be an integer just large enough so that $t_0^*>33766$ and $b(F,t_0^*)<\frac{1}{10}$.

Step 2 Estimate, via a constant-factor approximate counting algorithm of Stockmeyer [**Sto85**][26], both $N_F(t_0^*)$ and $\pi_F(t_0^*)$ within a factor of $\frac{9}{8}$, using polynomially many calls to our $\mathbf{NP}^{\mathbf{NP}}$ oracle. Call these approximations $\bar{N}$ and $\bar{\pi}$ respectively.

Step 3 If $\bar{N}\leq(\frac{9}{8})^2\bar{\pi}$, declare $Z_F\cap\mathbb{Q}^n$ empty. Otherwise, declare $Z_F\cap\mathbb{Q}^n$ nonempty. ■

That our algorithm runs in polynomial time follows easily from our quantitative estimates from theorem 12 and an analogous estimate for $N_F(x)$ (which also depends on GRH) from [**Roj00c**]. The same holds for the correctness of our algorithm.

Let us now close with some remarks on the strength of our last two theorems: First note that our restrictions on the input F are actually rather gentle. In particular, if one assumes $m\geq n$ and fixes the monomial term structure of F, then it follows easily from the theory of resultants [**GKZ94, Stu98, Roj99c**] that, for a generic choice of the coefficients, F will have only finitely many roots in $\mathbb{C}^n$. (See section 5 for our definition of generic.) Furthermore, it is quite frequently the case that our hypothesis involving Z_F and $\mathrm{Gal}(K/\mathbb{Q})$ holds when F fails to have a rational root.

THEOREM 14. [**Roj00c**, Thm. 4] *Following the notation above, fix the monomial term structure of F and assume further that $m\geq n$ and the coefficients of F*

[26] Stockmeyer's algorithm actually applies to any function from the complexity class #**P**, and it is easily verified that N_F and π_F lie within this class.

are integers of absolute value $\leq c$*. Then the fraction of such* F *with* $\mathrm{Gal}(K/\mathbb{Q})$ *acting transitively on* Z_F *is at least* $1-\mathcal{O}(\frac{\log c}{\sqrt{c}})$*. Furthermore, we can check whether* $\mathrm{Gal}(K/\mathbb{Q})$ *acts transitively on* Z_F *within* **EXPTIME** *or, if one assumes GRH, within* $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$. ■

Thus, if the monomial term structure of F is such that $\#Z_F \neq 1$ for a generic choice of the coefficients, it easily follows that at least a fraction of $1-\mathcal{O}(\frac{\log c}{\sqrt{c}})$ of the F specified above also have no rational roots. The case where the monomial term structure of F is such that $\#Z_F = 1$ for a generic choice of the coefficients is evidently quite rare, and will be addressed in future work.

Remark 3. *A stronger version of the* $m=n=1$ *case of theorem 14 (sans complexity bounds) was derived by Gallagher in* [**Gal73**]*. The* $m \geq n > 1$ *case follows from a combination of our framework here, the Lenstra-Lenstra-Lovasz (LLL) algorithm* [**LLL82**]*, and an effective version of Hilbert's Irreducibility Theorem from* [**Coh81**]. ■

As we have seen, transferring conditional speed-ups from $\mathbb{C}$ to $\mathbb{Q}$ presents quite a few subtleties, and these are covered at length in [**Roj00c**]. We also point out that there appears to be no obstruction to extending our algorithm above to detecting rational points over any fixed number field, within the same complexity bound. This will be pursued in future work.

4.1. Related Results Over $\mathbb{Q}$. We have mainly concentrated on the complexity of detecting rational points on certain zero-dimensional algebraic sets, which has been a somewhat overlooked topic. Indeed, while a **PSPACE** complexity bound for this problem could have been derived via, say, the techniques of [**CG84**] no later than 1984, there appears to be no explicit statement of this fact. In any event, that a large portion of this problem can be done within the polynomial hierarchy appears to be new.

On the other hand, for algebraic sets of positive dimension, even the decidability of feasibility over $\mathbb{Q}$ is open. That the study of rational points on higher-dimensional varieties has been, and continues to be, intensely studied by some of the best number theorists and algebraic geometers is a testament to the difficulty of this problem. Current work on finding rational points has thus focused on characterizing (in terms of the underlying complex geometry) when a variety has infinitely many rational points, and how and where density of rational points can appear.

For example, it was unproved until the work of Faltings in 1983 [**Fal84, Bom90**] that algebraic curves of genus[27] ≥ 2 have only finitely many rational points. (This fact was originally conjectured by L. J. Mordell in 1922.) The seminal work of Lang and Vojta has since lead to even deeper connections between the distribution of rational points and the geometry of the underlying complex manifold [**Voj87, Lan97**]. More recently, highly refined quantitative results (some depending on conjectures of Lang) on the density of rational points on certain varieties have appeared (see, e.g., [**Man95, Pac99, BT99**] and the references therein).

This is of course but a fragment of the wealth of current active research on rational points, and we have yet to speak of the complexity of finding integral points.

[27] We will use **geometric** (as opposed to arithmetic) genus throughout this paper. These definitions can be found in [**Har77, Mir95**].

5. Effective Siegel Versus Detecting Integral Points on Surfaces

The final results we present regard the computational complexity of certain problems involving integral points on varieties of dimension ≥ 1. We will strike a path leading to a relation between height bounds for integral points on algebraic plane curves and certain Diophantine prefixes in ≤ 4 variables, e.g., sentences of the form

$$\exists u \in \mathbb{N}\ \forall x \in \mathbb{N}\ \exists y \in \mathbb{N}\ f(u,x,y) \overset{?}{=} 0.$$

(The last sentence is an example of the prefix $\exists\forall\exists$, and we will casually refer to various quantified sentences in this way.) We then conclude with some evidence for the undecidability of Hilbert's Tenth Problem in three variables (theorem 20).

We first note that Diophantine complexity has quite a rich theory already in one variable.

Theorem 15. [**BCSS98**, Thm. 3, pg. 127] *Let $\tau(f)$ denote the SLP size of $f \in \mathbb{Z}[t]$, starting from the sequence $\{1, t, \dots\}$. Suppose there exists an absolute constant $C_2 > 0$ such that for all f, the number of integral roots of f is bounded above by $(\tau(f)+1)^{C_2}$. Then $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$.*[28] ■

In short, a deeper understanding of the SLP encoding (cf. section 3) over $\mathbb{Z}$ would have a tremendous impact in complexity theory.

Via the sparse encoding, the study of integral roots for polynomials in two variables leads us to similar connections with important complexity classes.

Theorem 16. [**AM75**] *Deciding whether $ax^2 + by = c$ has a root $(x,y) \in \mathbb{N}^2$, for an arbitrary input $(a,b,c) \in \mathbb{N}^3$, is **NP**-complete relative to the sparse encoding. i.e., there is an algorithm for this problem with bit complexity polynomial in* $\log(abc)$ *iff* $\mathbf{P} = \mathbf{NP}$. ■

Note that we hit the class **NP** rather quickly: quadratic polynomials (or genus zero curves)[29] are enough. The case of higher degree polynomials is much less understood. To see this, let us denote the following problem by HTP(n):

"Decide whether an arbitrary $f \in \mathbb{Z}[x_1, \dots, x_n]$ has a root in $\mathbb{N}^n$ or not."[30]

(So our last theorem can be rephrased as the **NP**-hardness of HTP(2) for quadratic polynomials.) It is then rather surprising that as of mid-2000, the decidability of HTP(2) is still open, even for general polynomials of degree 4 (or general curves of genus 2).

Alan Baker has conjectured [**Jon81**, Section 5] that the analogue HTP(2) for $\mathbb{Z}^2$ is decidable. More concretely, the decidability of HTP(2) is known in certain special cases, and these form a significant part of the applications of Diophantine approximation and arithmetic geometry. To describe the known cases, it is convenient to introduce the following functions.

Definition 1. *Following the notation of sections 2 and 3, define the function* $\mathrm{Big}_{\mathbb{N}} : \mathbb{Z}[x_1, x_2] \longrightarrow \mathbb{N} \cup \{0, \infty\}$ *by letting* $\mathrm{Big}_{\mathbb{N}}(f)$ *be the supremum of* $\max\{|r_1|, |r_2|\}$ *as (r_1, r_2) ranges over $\{(0,0)\} \cup (Z_f \cap \mathbb{N}^2)$. The function* $\mathrm{Big}_{\mathbb{Z}}(f)$ *is defined similarly, simply letting (r_1, r_2) range over $\{(0,0)\} \cup (Z_f \cap \mathbb{Z}^2)$ instead.* ■

[28] i.e., the analogue of the $\mathbf{P} \neq \mathbf{NP}$ conjecture for the BSS model over $\mathbb{C}$ would be settled.

[29] It will be convenient to describe bivariate polynomials in terms of their underlying complex geometry, and we will do so freely in this section.

[30] Hilbert's Tenth Problem in n variables is actually the simplification of HTP(n) where we seek roots in $\mathbb{Z}^n$. However, for technical reasons, it is more convenient to deal with HTP(n).

Parallel to HTP(n) and its analogue over $\mathbb{Z}^n$, the computability of $\mathrm{Big}_{\mathbb{N}}$ implies the computability of $\mathrm{Big}_{\mathbb{Z}}$. (Simply consider the substitution $f(x,y) \mapsto f(-x,-y)f(-x,y)f(x,-y)f(x,y)$.) The other direction is actually not trivial: there is nothing stopping a curve from having infinitely many integral points **outside** of the first quadrant, thus obstructing any useful bound for $\mathrm{Big}_{\mathbb{Z}}$ from being a useful bound for $\mathrm{Big}_{\mathbb{N}}$.

The computability of $\mathrm{Big}_{\mathbb{N}}$ would of course imply the decidability of HTP(2). However, as of mid-2000, even the computability of $\mathrm{Big}_{\mathbb{Z}}$ is, with a few exceptions, known only for those f where Z_f falls into one of the following cases: certain genus zero curves [**Pou93**], all genus one curves [**BC70**], certain genus two curves [**Gra94, Poo96**], Thue curves [**Bak68**], and curves in super-elliptic form [**Bak69, Bri84**]. (These also happen to be the only cases for which the decidability of HTP(2) is known.) For example, it is known that for any polynomial equation of the form

$$y^2 = a_0 + a_1x + a_2x^2 + a_3x^3,$$

where $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ and $a_0 + a_1x + a_2x^2 + a_3x^3$ has three distinct complex roots, all integral solutions must satisfy

$$|x|, |y| \leq \exp((10^6c)^{10^6}),$$

where c is any upper bound on $|a_0|, |a_1|, |a_2|, |a_3|$ [**Bak75**]. (More recent improvements of this bound can be found in [**Sch92**].)

Remark 4. *An interesting related conjecture of Steve Smale* [**Sma98**] *is that if a plane curve of positive genus has an integral point, then it must have an integral point of height singly exponential in the dense size of the defining polynomial. (See below for the definition of dense size.)* ■

Of course, one may still worry whether $\mathrm{Big}_{\mathbb{Z}}$ can be computable without $\mathrm{Big}_{\mathbb{N}}$ being computable. We can resolve this as follows:

Theorem 17. *The function* $\mathrm{Big}_{\mathbb{N}}$ *is computable* $\iff$ $\mathrm{Big}_{\mathbb{Z}}$ *is computable.*

The proof follows easily from theorem 22 of the next section, which describes the distribution of integral points within the real part of a complex curve. In spite of theorem 17, it is still unknown whether replacing $\mathbb{Z}^2$ by $\mathbb{N}^2$ makes a significant difference in the complexity of HTP(2). However, via theorem 21 of the next section, we can prove that a variant of HTP(2) is closely related to detecting infinitudes of integral points on plane curves.

Theorem 18. *Let* RatCurve(3) *denote the problem of deciding whether a (geometrically irreducible, possibly singular) genus zero curve in* $\mathbb{C}^3$ *defined over* $\mathbb{Z}$ *contains a point in* $\mathbb{N}^3$*. Also let* $\mathrm{HTP}^\infty(2)$ *denote the problem of deciding whether an arbitrary* $f \in \mathbb{Z}[x_1, x_2]$ *has infinitely many roots in* $\mathbb{N}^2$*. Then* RatCurve(3) *decidable* $\Longrightarrow$ $\mathrm{HTP}^\infty(2)$ *decidable.*

We note that the input for RatCurve(3) is given as usual: a set of polynomials in $\mathbb{Z}[x_1, x_2, x_3]$ defining the curve in question. Curiously, the decidability of RatCurve(3), $\mathrm{HTP}^\infty(2)$, and their analogues over $\mathbb{Z}$ are all unknown, in spite of Siegel's Theorem. (Siegel's Theorem [**Sie29**] is a famous result from 1934 partially classifying those curves with infinitely many integral points.) A refined version of Siegel's Theorem appears as theorem 21 of the next section.

The preceding results can all be considered as variations on the study of the Diophantine prefixes $\exists$ and $\exists\exists$. So to prove more decisive results it is natural to study subtler combinations of quantifiers. In particular, we will show that the prefix $\exists\forall\exists$ can be solved (almost always) within the polynomial hierarchy. To make this more precise, let us make two quantitative definitions: When we say that a statement involving a set of parameters $\{c_1,\ldots,c_N\}$ is true **generically**[31], we will mean that for any $M\in\mathbb{N}$, the statement fails for at most $\mathcal{O}(N(2M+1)^{N-1})$ of the $(c_1,\ldots,c_N)$ lying in $\{-M,\ldots,M\}^N$. Also, for an algorithm with a polynomial $f\in\mathbb{Z}[v,x,y]$ as input, speaking of the **dense encoding** will simply mean measuring the input size as $D+\sigma(f)$, where D (resp. $\sigma(f)$) is the total degree (resp. maximum bit-length of a coefficient) of f.

Theorem 19. [**Roj00c**] *Fix the Newton polytope Q of a polynomial $f\in\mathbb{Z}[v,x,y]$ and suppose that Q has at least one integral point in its interior.*[32] *Assume further that we measure input size via the dense encoding. Then, for a generic choice of coefficients depending only on Q, we can decide whether $\exists v\ \forall x\ \exists y\ f(v,x,y)=0$ (with all three quantifiers ranging over $\mathbb{N}$ or $\mathbb{Z}$) within* **coNP**. *Furthermore, we can check whether an input f has generic coefficients within* **NC**. ■

The hierarchy of complexity classes **NC** simply consists of those problems in **P** which admit efficient parallel algorithms (see [**Pap95**] for a full statement). Roughly speaking, deciding the prefix $\exists\forall\exists$ is equivalent to determining whether an algebraic surface has a slice (parallel to the (x,y)-plane) densely peppered with integral points, and we have thus shown that this problem is tractable for most inputs. Whether **coNP**-completeness persists relative to the **sparse** encoding remains an open question.

It is interesting to note that the exceptional case to our algorithm for $\exists\forall\exists$ judiciously contains an extremely hard number-theoretic problem: the prefix $\exists\exists$ or, equivalently, HTP(2). (That $\mathbb{Z}[v,y]$ lies in our exceptional locus is easily checked.) More to the point, James P. Jones has conjectured [**Jon81**] that the decidabilities of the prefixes $\exists\forall\exists$ and $\exists\exists$, quantified over $\mathbb{N}$, are equivalent. Thus, while we have not settled Jones' conjecture, we have at least shown that the decidability of $\exists\forall\exists$ now hinges on a sub-problem much closer to $\exists\exists$.

Call an algebraic surface $Z\subset\mathbb{C}^4$ **specially ruled** iff it is a bundle of genus zero curves fibered over a genus zero curve in the (u,v)-plane (coordinatizating $\mathbb{C}^4$ by (u,v,x,y)). The proof of theorem 19 is primarily based on a geometric trick which easily extends to the prefix $\exists\exists\forall\exists$. In particular, we also have the following result.

Theorem 20. *At least one of the following two statements is* **false***:*

1. *The function* $\mathrm{Big}_{\mathbb{N}}$ *is Turing-computable.*
2. *The Diophantine sentence*

$$\exists u\in\mathbb{N}\ \ \exists v\in\mathbb{N}\ \ \forall x\in\mathbb{N}\ \ \exists y\in\mathbb{N}\ \ f(u,v,x,y)\overset{?}{=}0$$

is decidable in the special case where the underlying 3-fold Z_f contains a specially ruled surface.

In particular, HTP(3) *is a special case of the problem mentioned in statement (2).*

A slightly stronger version of theorem 20 appears in [**Roj00a**] and, for the convenience of the reader, we supply a more streamlined proof in section 6.2.3. We thus

[31] We can in fact assert a much stronger condition, but this one suffices for our present purposes.

[32] So, among other things, we are assuming Q is 3-dimensional.

now have (applying theorem 17) a weak version of the following implication: $\mathrm{Big}_{\mathbb{Z}}$ computable $\Longrightarrow$ HTP(3) undecidable.

Since Matiyasevich and Robinson have shown that $\exists\exists\forall\exists$ is undecidable (when all quantifiers range over $\mathbb{N}$) [**MR74**], our last theorem can also be interpreted as a restriction of this undecidability to a particular subset of the general problem. Whether this subproblem can be completely reduced to HTP(3) is therefore of the utmost interest.

5.1. Related Work Over $\mathbb{N}$ and $\mathbb{Z}$.

We first point out that the decidability of $\exists\forall\exists$ was an open problem and, in spite of theorem 19, remains open for **arbitrary** inputs. We also note that our algorithm for (most of) $\exists\forall\exists$ is based on an important result of Tung for the prefix $\forall\exists$.

Tung's Theorem. [**Tun87**] *Deciding the quantifier prefix $\forall\exists$ (with all quantifiers ranging over $\mathbb{N}$ or $\mathbb{Z}$) is* **coNP***-complete relative to the dense encoding.* ■

The decidability of $\forall\exists$ (over $\mathbb{N}$ and $\mathbb{Z}$) was first derived by James P. Jones in 1981 [**Jon81**]. The algorithms for $\forall\exists$ alluded to in Tung's Theorem are based on some very elegant algebraic facts due to Jones, Schinzel, and Tung. We illustrate one such fact for the case of $\forall\exists$ over $\mathbb{N}$.

The JST Theorem. [**Jon81, Sch82, Tun87**] *Given any $f \in \mathbb{Z}[x,y]$, we have that $\forall x\ \exists y\ f(x,y)=0$ iff all three of the following conditions hold:*

1. *The polynomial f factors into the form $f_0(x,y)\prod_{i=1}^{j}(y-f_i(x))$ where $f_0(x,y) \in \mathbb{Q}[x,y]$ has* **no** *zeroes in the ring $\mathbb{Q}[x]$, and for all i, $f_i \in \mathbb{Q}[x]$ and the leading coefficient of f_i is positive.*
2. *$\forall x \in \{1,\ldots,x_0\}\ \exists y \in \mathbb{N}$ such that $f(x,y)=0$, where $x_0 = \max\{s_1,\ldots,s_j\}$, and for all i, s_i is the sum of the squares of the coefficients of f_i.*
3. *Let α be the least positive integer such that $\alpha f_1,\ldots,\alpha f_j \in \mathbb{Z}[x]$ and set $g_i := \alpha f_i$ for all i. Then the* **union** *of the solutions of the following j congruences $g_1(x) \equiv 0 \pmod{\alpha},\ldots,g_j(x) \equiv 0 \pmod{\alpha}$ is* **all** *of $\mathbb{Z}/\alpha\mathbb{Z}$.* ■

The analogue of the JST Theorem over $\mathbb{Z}$ is essentially the same, save for the absence of condition (2), and the removal of the sign check in condition (1) [**Tun87**].

The study of the decidability of Diophantine prefixes dates back to [**Mat73, MR74, Jon81**], and [**Mat93, Tun99, Roj99b, Roj00c**] give some of the most recent results. Of course, as we have seen above, there is still much left to be done, and we hope that this paper sparks the interests of other researchers.

In particular, the precise complexity of checking whether an input $f \in \mathbb{Z}[u,v,x,y]$ satisfies the hypothesis of statement (2) of theorem 20 is unknown. (The decidability of this problem is at least known, and there are more restricted versions of (2) which can be checked within **NC** [**Roj00a**].) The author conjectures that this hypothesis can in fact be decided within **NC**, relative to the dense encoding.

More to the point, it is curious that the complexity of deciding whether a given curve has infinitely many integral points is also open. The best result along these lines is the following refined version of Siegel's Theorem:

Theorem 21. [**Sil00**] *Following the notation of sections 2 and 3, suppose $f \in \mathbb{Z}[x_1,x_2]$ is such that Z_f is a geometrically irreducible curve. Then $Z_f \cap \mathbb{Z}^2$ is infinite $\Longleftrightarrow$ all of the following three conditions are satisfied:*

(a) *Z_f has genus 0,*

(b) *$Z_f \cap \mathbb{Z}^2$ contains at least one non-singular point, and*

(c) *the highest degree part of f has either (i) exactly one root in $\mathbb{P}^1_{\mathbb{C}}$ (necessarily rational) or (ii) has exactly two distinct roots in $\mathbb{P}^1_{\mathbb{C}}$* **and** *they are both real.* ■

Joseph H. Silverman has pointed out that this result may already be known to experts in algebraic curves. Another curious fact regarding Siegel's theorem is that it still has no proof which settles the computability of $\mathrm{Big}_{\mathbb{Z}}$.

A useful result arising from Silverman's proof of theorem 21 is the following solution to a conjecture of the author from [**Roj00a**]:

THEOREM 22. [**Sil00**] *Let W be any geometrically irreducible curve in $\mathbb{C}^2$ defined over $\mathbb{Z}$ possessing infinitely many integral points. Let W' be any unbounded subset of $W \cap \mathbb{R}^2$. Then W' contains infinitely many integral points.* ■

This result, combined with a little computational algebraic geometry, provides the proof of theorem 17 and the details appear in section 6.2.

As for more general relations between HTP(n) and its analogue over $\mathbb{Z}^n$, it is easy to see that the decidability of HTP(n) implies the decidability of its analogue over $\mathbb{Z}^n$. Unfortunately, the converse is currently unknown. Via Lagrange's Theorem (that any positive integer can be written as a sum of four squares) one can easily show that the **un**decidability of HTP(n) implies the **un**decidability of the analogue of HTP($4n$) over $\mathbb{Z}^n$. More recently, Zhi-Wei Sun has shown that the $4n$ can be replaced by $2n+2$ [**Sun92**].

6. Proofs of Our Main Technical Results

For the convenience of the reader, let us briefly distinguish what is new and/or recent: To the best of the author's knowledge, theorems 2, 4, 5, 6, 7, 17, and 18, and corollary 1 have not appeared in print before. Also, although theorem 17 was conjectured, along with a plan of attack, in [**Roj00a**], its full proof has not appeared before. Finally, while preliminary versions of theorems 5 and 7 appeared earlier in [**Roj99c**], their corresponding height bounds are new.

As for the remaining results, they have either already appeared, or are about to appear, in the references listed in their respective statements.

Our proofs will thus focus on results over our "outlying" rings: $\mathbb{C}$ and $\mathbb{Z}$.

6.1. Proofs of Our Results Over $\mathbb{C}$: Theorems 2, 5, 6, 7, and 4.

While our proof of theorem 4 will not directly require knowledge of resultants, our proofs of theorems 2, 5, 6, and 7 are based on the **toric resultant**.[33] This operator allows us to reduce all the computational algebraic geometry we will encounter to matrix and univariate polynomial arithmetic, with almost no commutative algebra machinery. We supply a precis on the toric resultant in the following section.

As mentioned earlier, we will reduce the description of Z_F to univariate polynomial factorization. Another trick we will use is to reduce most of our questions to finding isolated roots of polynomial systems where the numbers of equations and variables is the same.

[33] Other commonly used prefixes for this modern generalization of the classical resultant [**Van50**] include: sparse, mixed, sparse mixed, $\mathcal{A}$-, $(\mathcal{A}_1, \ldots, \mathcal{A}_k)$-, and Newton. Resultants actually date back to work Cayley and Sylvester in the $19^{\underline{\text{th}}}$ century, but the toric resultant incorporates some combinatorial advances from the late $20^{\underline{\text{th}}}$ century.

These geometric constructions are useful for the proof of theorem 4 as well, but more in a theoretical sense than in an algorithmic sense. As we will see in section 6.1.6, it is number theory which allows us to enter a lower complexity class, and univariate reduction is needed only for quantitative estimates.

6.1.1. *Background on Toric Resultants.*

Since we do not have the space to give a full introduction to resultants we refer the reader to [**Emi94, GKZ94, Stu98**] for further background. The necessary facts we need are all summarized below. In what follows, we let $[j]:=\{1,\ldots,j\}$.

Recall that the **support**, **Supp(f)**, of a polynomial $f\in\mathbb{C}[x_1,\ldots,x_n]$ is simply the set of exponent vectors of the monomial terms appearing[34] in f. The support of the **polynomial system** $F=(f_1,\ldots,f_m)$ is simply the m-tuple **Supp(F)** $:=(\mathrm{Supp}(f_1),\ldots,\mathrm{Supp}(f_m))$. Let $\bar{\mathcal{A}}=(\mathcal{A}_1,\ldots,\mathcal{A}_{m+1})$ be any $(m+1)$-tuple of non-empty finite subsets of $\mathbb{Z}^n$ and set $\mathcal{A}:=(\mathcal{A}_1,\ldots,\mathcal{A}_m)$. If we say that F has **support contained in** $\mathcal{A}$ then we simply mean that $\mathrm{Supp}(f_i)\subseteq\mathcal{A}_i$ for all $i\in[m]$.

Definition 2. *Following the preceding notation, suppose we can find line segments* $[v_1,w_1],\ldots,[v_{m+1},w_{m+1}]$ *with* $\{v_i,w_i\}\subseteq\mathcal{A}_i$ *for all* i *and* $\mathrm{Vol}_m(L)>0$*, where* L *is the convex hull of* $\{\mathbf{O},w_1-v_1,\ldots,w_{m+1}-v_{m+1}\}$*. Then we can associate to* $\bar{\mathcal{A}}$ *a unique (up to sign) irreducible polynomial* $\mathrm{Res}_{\bar{\mathcal{A}}}\in\mathbb{Z}[c_{i,a} \mid i\in[m+1]\ ,\ a\in\mathcal{A}_i]$ *with the following property: If we identify* $\bar{\mathcal{C}}:=(c_{i,a} \mid i\in[m+1]\ ,\ a\in\mathcal{A}_i)$ *with the vector of coefficients of a polynomial system* $\bar{F}$ *with support contained in* $\bar{\mathcal{A}}$ *(and constant coefficients), then* $\bar{F}$ *has a root in* $(\mathbb{C}^*)^n \Longrightarrow \mathrm{Res}_{\bar{\mathcal{A}}}(\bar{\mathcal{C}})=0$*. Furthermore, for all* i*, the degree of* $\mathrm{Res}_{\bar{\mathcal{A}}}$ *with respect to the coefficients of* f_i *is no greater than* V_F*.* ■

We emphasize that the implication above does **not** go both ways: the correct converse involves toric varieties [**GKZ94, Roj99a, Roj99c**]. A consequence of the above definition is that the toric resultant applies mainly to systems of $n+1$ polynomials in n variables. However, via a trick from the next section, this will cause no significant difficulties when we consider m polynomials in n variables.

That the toric resultant can actually be defined as above is covered in detail in [**Stu94, GKZ94**]. There is in fact an exact formula for the degree of Res with respect to the coefficients of f_i involving **mixed** volumes [**Stu94, GKZ94**]. Our simplified upper bound follow easily from the fact that mixed volume never decreases when the input polytopes are grown [**BZ88**].

Another operator much closer to our purposes is the **toric perturbation** of F.

Definition 3. *Following the notation of definition 2, assume further that* $m=n$*,* $\mathrm{Supp}(F)=\mathcal{A}$*, and* $\mathrm{Supp}(F^*)\subseteq\mathcal{A}$*. We then define*

$$\mathrm{Pert}_{(F^*,\mathcal{A}_{n+1})}(u)\in\mathbb{C}[u_a \mid a\in\mathcal{A}_{n+1}]$$

to be the coefficient of the term of

$$\mathrm{Res}_{\bar{\mathcal{A}}}(f_1-sf_1^*,\ldots,f_n-sf_n^*,\sum_{a\in\mathcal{A}_{n+1}}u_ax_a)\in\mathbb{C}[s][u_a \mid a\in\mathcal{A}_{n+1}]$$

of **lowest** *degree in* s*.* ■

[34] We of course fix an ordering on the coordinates of the exponents which is compatible with the usual ordering of $x_1,\ldots,x_n$.

The constant term of the last resultant is a generalization of the classical **Chow form** of a zero-dimensional variety [**Van50**]. The consideration of the higher order coefficients is necessary when Z_F is positive-dimensional. In particular, the geometric significance of Pert can be summarized as follows: For a suitable choice of F^*, $\mathcal{A}_{n+1}$, and $\{u_a\}$, Pert satisfies all the properties of the polynomial h_F from theorem 5 in the special case $m=n$. In essence, Pert is an algebraic deformation which allows us to replace the positive-dimensional part of Z_F by a finite subset which is much easier to handle.

To prove theorems 2, 5, and 7 we will thus need a good complexity estimate for computing Res and Pert.

LEMMA 1. *Following the notation above, let $\mathcal{R}_F$ (resp. $\mathcal{P}_F$) be the number of deterministic arithmetic operations needed to evaluate* $\mathrm{Res}_{\bar{\mathcal{A}}}$ *(resp.* $\mathrm{Pert}_{(F^*,\mathcal{A}_{n+1})}$*) at any point in $\mathbb{C}^{k+n+1}$ (resp. $\mathbb{C}^{2k+n+1}$), where $\mathcal{A}\subseteq\mathrm{Supp}(F)$ and $\mathcal{A}_{n+1}:=\{\mathbf{O},e_1,\ldots,e_n\}$. Also let r_F be the total degree of* $\mathrm{Res}_{\bar{\mathcal{A}}}$ *as a polynomial in the coefficients of $\bar{F}$ Then $r_F\leq(n+1)V_F$, $\mathcal{R}_F\leq(n+1)r_F\mathcal{O}(M_F^{2.376})$, and $\mathcal{P}_F\leq(r_F+1)\mathcal{R}_F+r_F(1+\frac{3}{2}\log r_F)$. Furthermore, $k\leq m(V_F+n)$ and $M_F\leq e^{1/8}\frac{e^n}{\sqrt{n+1}}V_F+\prod_{i=1}^{n}(p_i+2)-\prod_{i=1}^{n}(p_i+1)$, where p_i is the length of the projection of nQ_F onto the x_i-axis. (Note that $e^{1/8}\approx1.3315$.)* ■

Proof: The bound on $\mathcal{R}_F$ (resp. $\mathcal{P}_F$) follows directly from [**EC93**] (resp. [**Roj99c**]), as well as a basic complexity result on the **inverse discrete Fourier transform** [**BP94**, pg. 12].

The bound on k follows by noting that $k\leq m\ell_F$, where ℓ_F is the number of lattice points in the polytope Q_F. By a classical lattice point count of Blichfeldt [**Bli21**], we obtain $\ell_F\leq V_F+n$ and we are done.

As for the bound on M_F, we will observe a bit later that M_F can be bounded above by the number of lattice points in the **Minkowski sum**[35] $Q'_F:=nQ_F+\mathrm{Conv}\{\mathbf{O},e_1,\ldots,e_n\}$. (This polytope is clearly contained in the polytope $(n+1)Q_F$ mentioned in theorem 2.) Noting that $\frac{(n+1)^n}{n!}\leq e^{1/8}\frac{e^n}{\sqrt{n+1}}$ via Stirling's estimate [**Rud76**, pg. 200], and that the length of the projection of Q'_F onto the x_i-axis is exactly p_i+1, our bound on M_F follows immediately from another simple lattice point count [**GW93**, Formula 3.11]. ■

REMARK 5. *That $M_F=\mathcal{O}(V_F)$ for fixed n is immediate from our last lemma. Note also that Q'_F is contained in the standard n-simplex scaled by a factor $nD+1$. Calling the latter polytope $\mathcal{Q}_F$, it is clear that the number of lattice points in $\mathcal{Q}_F$ is yet another upper bound on M_F. The latter lattice point count in turn has a simple explicit formula in terms of the binomial coefficient, and this is how we derived the crude bound on M_F mentioned in section 2.1.* ■

Admittedly, such complexity estimates seem rather mysterious without any knowledge of how Res and Pert are computed. So let us now give a brief summary: The key fact to observe is that, in the best circumstances, one can express Res as the determinant of a (square) sparse structured matrix $\mathcal{M}_{\bar{\mathcal{A}}}$ — a **toric resultant matrix** — whose entries are either 0 or polynomials in the coefficients of $\bar{F}$. (In fact, the $\mathcal{M}_{\bar{\mathcal{A}}}$ we use will have every row equal to a permutation of the vector $v=(\mathcal{C}_i,0,\ldots,0)$, where $\mathcal{C}_i$ is the vector of coefficients of f_i and i (and the permutation) depends on the row.) These matrices have their origin in the study of

[35] The Minkowksi sum of any two subsets $A,B\subseteq\mathbb{R}^n$ is simply the set $\{a+b \mid a\in A\ ,\ b\in B\}$.

certain spectral sequences [**GKZ94**] and there are now down-to-earth combinatorial algorithms for finding them [**EC93, Emi94, EP99, EM99**].

So the quantity M_F in our theorems is nothing more than the number of rows (or columns) of $\mathcal{M}_{\bar{\mathcal{A}}}$. The bound on M_F from our last theorem thus arises simply by applying the main algorithm from [**EC93**], and observing that this particular construction of $\mathcal{M}_{\bar{\mathcal{A}}}$ creates a matrix row for every lattice point in a translate of the polytope $\mathrm{Conv}(\mathcal{A}_1+\cdots+\mathcal{A}_{n+1})$. In particular, it is also the case that the deterministic arithmetic complexity of constructing $\mathcal{M}_{\bar{\mathcal{A}}}$ is dominated by $\mathcal{O}(M_F\log n+n^2)$ [**Roj00d**], so we can henceforth ignore this construction in our complexity bounds. Better still, the quantity M_F can be expected to admit even sharper upper bounds, once better algorithms for building toric resultant matrices are found.

However, it is more frequently the case that Res is but a **divisor** of $\det \mathcal{M}_{\bar{\mathcal{A}}}$, and further work must be done. Fortunately, in [**EC93, Emi94**], there are general randomized and deterministic algorithms for extracting Res. These algorithms work via subtle refinements of the classical technique of recovering the coefficients of a polynomial g of degree D by evaluating g at $D+1$ points and then solving for the coefficients via a structured linear system. This accounts for the appearance of the famous linear algebra complexity exponent ($\omega<2.376$), or simple functions thereof, in our complexity estimates.

6.1.2. *The Proof of Theorem 2.*

Our algorithm can be stated briefly as follows:

Step 0 If f_i is indentically 0 for all i, declare that Z_F has dimension n and stop. Otherwise, let $i:=n-1$.

Step 1 For each $j\in[2k+1]$, compute an $(i+1)n$-tuple of integers $(\varepsilon_1(j),\ldots,\varepsilon_n(j),\varepsilon_{(1,1)}(j),\ldots,\varepsilon_{(i,n)}(j))$ via lemma 2 and the polynomial system (3) below.

Step 2 Via theorem 5, check if the polynomial system

$$\begin{array}{rcl}\varepsilon_1(j)f_1+\cdots+\varepsilon_1(j)^m f_m+\varepsilon_1(j)^{m+1}l_1+\cdots+\varepsilon_1(j)^{m+i}l_i & = & 0\\ & \vdots & \\ \varepsilon_n(j)f_1+\cdots+\varepsilon_n(j)^m f_m+\varepsilon_n(j)^{m+1}l_1+\cdots+\varepsilon_n(j)^{m+i}l_i & = & 0\end{array} \tag{3}$$

has a root for more than half of the $j\in[2k+1]$, where $l_t:=\varepsilon_{(t,1)}x_1+\cdots+\varepsilon_{(t,n)}x_n$.

Step 3 If so, declare that Z_F has dimension i and stop. Otherwise, if $i\geq 1$, set $i\mapsto i-1$ and go to Step 1.

Step 4 Via theorem 7 and a univariate gcd computation, check if the system (3) has a root which is also a root of F.

Step 5 If so, declare that Z_F has dimension 0 and stop. Otherwise, declare Z_F empty and stop.

Before analyzing the correctness of our algorithm, let us briefly clarify Steps 2 and 4. First let $G_{(j)}$ denote the polynomial system (3). In Step 2, we apply theorem 5 to calculate the polynomial $h_{G_{(j)}}$. Since the $G_{(j)}$ all have an equal number of variables and equations (and none of the equations is of the form $0=0$), assertion (1) of theorem 5 tells us that a particular $G_{(j)}$ has a complex root iff $h_{G_{(j)}}$ has positive degree. So it suffices to compute $h_{G_{(j)}}$ to check the feasibility of $G_{(j)}$. As for Step 4, note that thanks to theorem 7, $G_{(j)}$ has a root in common with F iff $\gcd\{h_{G_{(j)}},g_1(h_1,\ldots,h_n),\ldots,g_n(h_1,\ldots,h_n)\}$ has positive degree, where $h_1, \ldots, h_n$ are the polynomials corresponding to the application of theorem 7 to $G_{(j)}$. The preceding gcd and composition of univariate polynomials can be computed within $\mathcal{O}(nk(n \log D)V_F \log^2 V_F)$ arithmetic operations via standard univariate polynomial algorithms [**BP94**], and we will soon see that this complexity is negligible compared to the work performed in the rest of our algorithm.

Let us now check the correctness of our algorithm: Via lemma 2 and theorem 5, we see that Step 2 gives a "yes" answer iff the intersection of $Z_{\tilde{F}}$ with a generic codimension i flat is finite (and nonempty), where $\tilde{F}$ is an n-tuple of generic linear combinations of the f_i. Thus Step 2 gives a "yes" answer iff $\dim Z_{\tilde{F}} = i$. Lemma 6 below tells us that $\dim Z_F = \dim Z_{\tilde{F}}$ if $\dim Z_F \geq 1$. Otherwise, Step 5 correctly decides whether Z_F is empty whenever Z_F is finite. Thus the algorithm is correct.

As for the complexity of our algorithm, letting $\mathcal{S}$ (resp. $\mathcal{U}$, $\mathcal{U}'$) be the complexity of the corresponding application of lemma 2 (resp. theorems 5 and 7), we immediately obtain a deterministic arithmetic complexity bound of

$$(n-2)\mathcal{S} \quad \text{(All Executions of Step 1)}$$

$$+(n-2)(2k+1)\mathcal{U} \quad \text{(All Executions of Step 2)}$$

$$+\mathcal{U}' + \mathcal{O}(n^2 k V_F (\log^2 V_F)(\log D)) \quad \text{(Step 4)}$$

(The complexity of the "if" statements in Steps 3 and 5 is negligible.) Remark 7 below tells us that $\mathcal{S} = \mathcal{O}((k+n^2)\log(m+n))$. Furthermore, in the proofs of theorems 7 and 5 (cf. sections 6.1.5 and 6.1.3) later we will see that $\mathcal{U}' = \mathcal{O}(n\mathcal{U})$ and $\mathcal{U} = \mathcal{O}(V_F^3 \mathcal{P}_F)$. Since $k \geq m$, our overall complexity bound becomes $\mathcal{O}(nk\mathcal{U} + n\mathcal{S}) = \mathcal{O}(nkV_F^3\mathcal{P}_F + n(k+n^2)\log(m+n)) = \mathcal{O}(n^4 k M_F^{2.376} V_F^5 + n(k+n^2)\log(m+n)) = \mathcal{O}(n^4 k M_F^{2.376} V_F^5 + nk\log(m+n))$. ■

Remark 6. *Note that if we somehow know that* $\dim Z_F \geq 1$*, then we do not need assertion (2) of theorem 5, nor do we need to apply theorem 7. We can thus pick any integral point (not equal to* $\mathbf{O}$*) for* u_F *and skip one of the steps of the proof of theorem 5. This removes a factor of* V_F^2 *from the first (usually dominant) summand of our complexity bound.* ■

Lemma 2. *Suppose* $G(w,v)$ *is a formula of the form*

$$\exists x_1 \in \mathbb{C} \cdots \exists x_n \in \mathbb{C}\ (g_1(x,w,v)=0) \wedge \cdots \wedge (g_s(x,w,v)=0),$$

where $g_1, \ldots, g_s \in \mathbb{C}[x_1, \ldots, x_n, w_1, \ldots, w_k, v_1, \ldots, v_r]$*. Then there is a sequence* $v(1), \ldots, v(2k+1) \in \mathbb{C}^r$ *such that for all* $w \in \mathbb{C}^k$*, the following statement holds:* $G(w, v(j))$ *is true for at least half of the* $j \in [2k+1] \iff G(w,v)$ *is true for a Zariski-open set of* $v \in \mathbb{C}^r$*. Furthermore, this sequence can be computed within* $\log\sigma + (k+n+r)\log D$ *arithmetic operations, where* σ *(resp. D) is the maximum bit-size of any coefficient (resp. maximum degree) of any* g_i*.* ■

The above lemma is actually just a special case of theorem 5.6 of [**Koi97**].

Remark 7. *For the proof of theorem 2, we have* $s := n$*,* $(g_1, \ldots, g_s) := G_{(j)}$*,* $r := (i+1)n \leq (n-1)n$*,* $v(j) = (\varepsilon_1(j), \ldots, \varepsilon_n(j), \varepsilon_{(1,1)}(j), \ldots, \varepsilon_{(i,n)}(j))$*, and we take* w *to be the vector of coefficients of* F*. We thus obtain* $\sigma = 1$ *and* $D = m+i+1 \leq m+n$*.* ■

6.1.3. *The Proof of Theorem 5.*
Curiously, precise estimates on coefficient growth in toric resultants are absent from the literature. So we supply such an estimate below. In what follows, we use u_i in place of u_{e_i}.

Theorem 23. *Following the notation of lemma 1, suppose the coefficients of F (resp. F^*) have absolute value bounded above by c (resp. c^*) for all $i \in [n]$ and $u_1, \ldots, u_n \in \mathbb{C}$. Also let $\|u\| := \sqrt{u_1^2 + \cdots + u_n^2}$ and let μ denote the maximal number of monomial terms in any f_i. Then the coefficient of u_0^i in $\mathrm{Pert}_{(F^*, \mathcal{A}_{n+1})}$ has absolute value bounded above by*

$$\frac{e^{13/12}}{\sqrt{\pi}} \sqrt{M_F + 1} \cdot 4^{M_F - i/2} \|u\|^{V_F - i} (\sqrt{\mu}(c + c^*))^{M_F} \binom{V_F}{i},$$

assuming that $\det \mathcal{M}_{\bar{\mathcal{A}}} \neq 0$ *under the substitution* $(F - sF^*, u_0 + u_1 x_1 + \cdots + u_n x_n) \mapsto \bar{F}$. *(Note also that* $\frac{e^{13/12}}{\sqrt{\pi}} \approx 1.66691$.*)*

Proof: Let c_{ij} denote the coefficient of $u_0^i s^j$ in $\det \mathcal{M}_{\bar{\mathcal{A}}}$, under the substitution $(F - sF^*, u_0 + u_1 x_1 + \cdots + u_n x_n) \mapsto \bar{F}$. Our proof will consist of computing an upper bound on $|c_{ij}|$, so we can conclude simply by maximizing over j and then invoking a quantitative lemma on factoring.

To do this, we first observe that one can always construct a toric resultant matrix with exactly n_F rows corresponding to f_{n+1} (where $\delta(Z_F) \leq n_F \leq V_F$), and the remaining rows corresponding to $f_1, \ldots, f_n$. (This follows from the algorithms we have already invoked in lemma 1.) Enumerating how appropriate collections rows and columns can contain i entries of u_0 (and j entries involving s), it is easily verified that c_{ij} is a sum of no more than $\binom{V_F}{i} \binom{M_F - i}{j}$ subdeterminants of $\mathcal{M}_{\bar{\mathcal{A}}}$ of size no greater than $M_F - i - j$. The coefficient c_{ij} also receives similar contributions from some larger subdeterminants since the rows of $\mathcal{M}_{\bar{\mathcal{A}}}$ corresponding to $f_1, \ldots, f_n$ involve terms of the form $\eta + \nu s$.

Via lemma 3 below, we can then derive an upper bound of

$$\binom{V_F}{i} \binom{M_F - i}{j} \|u\|^{V_F - i} (\sqrt{\mu}(c + c^*))^{M_F - j}$$

on $|c_{ij}|$. However, what we really need is an estimate on the coefficient c_i of u_0^i of $\mathrm{Pert}_{(F^*, \mathcal{A}_{n+1})}$, assuming the non-vanishing of $\det \mathcal{M}_{\bar{\mathcal{A}}}$. To estimate c_i, we simply apply lemma 4 below (observing that $\mathrm{Pert}_{(F^*, \mathcal{A}_{n+1})}$ is a divisor of an $M_F \times M_F$ determinant) to obtain an upper bound of

$$\sqrt{M_F + 1} \cdot 2^{M_F} \binom{V_F}{i} \max_j \left\{ \binom{M_F - i}{j} \right\} \|u\|^{V_F - i} (\sqrt{\mu}(c + c^*))^{M_F}$$

on $|c_i|$. We can then finish via the elementary inequality $\binom{M_F - i}{j} \leq \frac{e^{13/12}}{\sqrt{\pi}} 2^{M_F - i}$, valid for all j (which in turn is a simple corollary of Stirling's formula). ■

A simple result on the determinants of certain symbolic matrices, used above, is the following.

Lemma 3. *Suppose A and B are complex $N \times N$ matrices, where B has at most N' nonzero rows. Then the coefficient of s^j in $\det(A + sB)$ has absolute value* *no greater than* $\binom{N'}{j} v^{N-j}(v+w)^j$*, where* v *(resp.* w*) is any upper bound on the Hermitian norms of the rows of* A *(resp.* B*).* ■

The lemma follows easily by reducing to the case $j=0$, via the multilinearity of the determinant. The case $j=0$ is then nothing more than the classical **Hadamard's lemma** [**Mig92**].

The lemma on factorization we quoted above is the following.

Lemma 4. [**Mig92**] *Suppose* $f \in \mathbb{Z}[x_1,\ldots,x_N]$ *has total degree* D *and coefficients of absolute value* $\leq c$*. Then* $g \in \mathbb{Z}[x_1,\ldots,x_N]$ *divides* $f \Longrightarrow$ *the coefficients of* g *have absolute value* $\leq \sqrt{D+1}\cdot 2^D c$*.* ■

We are now ready to prove theorem 5:

Proof of Theorem 5:

By adjusting the number polynomials m we can immediately assume that no f_i is indentically zero. Furthermore, if $m=0$, we can clearly set $h:=0$. So we can also assume that $m\geq 1$. We now consider three obvious cases.

(The Case $m=n$): The existence of an h_F satisfying (0)–(5) will follow from setting $h_F(u_0) := \mathrm{Pert}_{(F^*,\mathcal{A}_{n+1})}(u_0)$ for $\mathcal{A}_{n+1}$ as in lemma 1, F^* as in lemma 5 below, and picking several $(u_1,\ldots,u_n)$ until a good one is found. Assertion (0) of theorem 5 thus follows trivially. That the conclusion of lemma 5 implies assertion (1) is a consequence of [**Roj99c**, Def. 2.2 and Main Theorem 2.1].

To prove assertions (1)–(5) together we will then need to pick $(u_1,\ldots,u_n)$ subject to a final technical condition. In particular, consider the following method: Pick $\varepsilon\in[1+\binom{V_F}{2}]$ and set $u_i:=\varepsilon^i$ for all $i\in[n]$. The worst that can happen is that a root of h_F is the image two distinct points in Z_F under the map $(\zeta_1,\ldots,\zeta_n)\mapsto u_1\zeta_1+\cdots+u_n\zeta_n$, thus obstructing assertion (2). (Whether this happens can easily be checked within $\mathcal{O}(V_F \log V_F)$ arithmetic operations via a gcd calculation detailed in [**Roj99c**, Sec. 5.2], after first finding the coefficients of h_F.) Otherwise, it easily follows from Main Theorems 2.1 and 2.4 of [**Roj99c**] (and theorem 7 above and theorem 23 below) that h_F satisfies assertions (1)–(3) and (5).

Since there are at most $\binom{V_F}{2}$ pairs of points (ζ_1,ζ_2), picking $(u_1,\ldots,u_n)$ as specified above **will** eventually give us a good $(u_1,\ldots,u_n)$. The overall arithmetic complexity of our search for u_F and h_F is, thanks to lemma 1, $(\binom{V_F}{2}+1)\cdot(V_F\mathcal{P}_F+\mathcal{O}(V_F\log V_F))$. This proves assertion (4), and we are done. ■

Remark 8. *Note that we never actually had to compute* V_F *above: To pick a suitable* u*, we simply keep picking choices (in lexicographic order) with successively larger and larger coodinates until we find a suitable* u*.* ■

(The Case $m<n$): Take $f_{n+1}=\cdots=f_m=f_n$. Then we are back in the case $m=n$ and we are done. ■

(The Case $m>n$): Here we employ an old trick: We substitute generic linear combinations of $f_1,\ldots,f_m$ for $f_1,\ldots,f_n$. In particular, set $\tilde{f_i} := f_1+\varepsilon_i f_2+\cdots+\varepsilon_i^{m-1}f_m$ for all $i\in[n]$. It then follows from lemma 6 below that, for generic $(\varepsilon_1,\ldots,\varepsilon_n)$, $Z_{\tilde{F}}$ is the union of Z_F and a (possibly empty) finite set of points. So by the $m\!=\!n$ case, and taking into account the larger value for c in our application of theorem 23, we are done. $\blacksquare$

Remark 9. *Following the notation of theorem 23, we thus see that the asymptotic bound of assertion (3) can be replaced by an explicit bound of*

$$\log\left\{\frac{e^{13/6}}{\pi}\sqrt{M_F+1}\cdot 2^{V_F}4^{M_F}\left(\sqrt{n}\left(\binom{V_F}{2}+1\right)^n\right)^{V_F}(c+1)^{M_F}\right\}$$

if $m\!\leq\! n$*, or*

$$\log\left\{\frac{e^{13/6}}{\pi}\sqrt{M_F+1}\cdot 2^{V_F}4^{M_F}\left(\sqrt{n}\left(\binom{V_F}{2}+1\right)^n\right)^{V_F}\sqrt{\mu}^{M_F}(m(mV_F+1)^{m-1}c+1)^{M_F}\right\}$$

for $m\!>\!n\!\geq\!1$*.* $\blacksquare$

Lemma 5. *Following the notation above let* $\mathcal{A}^*_i\!=\!\{\mathbf{O},e_1,\ldots,e_n\}\cup\bigcup^n_{j=1}\mathcal{A}_j$ *for all* $i\in[n]$ *and* $k^*:=n\#\mathcal{A}_1$*, where* $\#$ *denotes set cardinality. Also let* $\mathcal{C}^*$ *be the coefficient vector of* F^**. Then there is an* F^* *such that (i)* $\mathrm{Supp}(F^*)\subseteq\mathcal{A}^*$*, (ii)* $\mathcal{C}^*\!=\!(1,\ldots,1)$*, (iii)* F^* *has exactly* V_F *roots in* $(\mathbb{C}^*)^n$ *counting multiplicities, and (iv)* $\det\mathcal{M}_{\bar{\mathcal{A}}}\!\neq\!0$ *under the substitution* $(F-sF^*,u_0+u_1x_1+\cdots+u_nx_n)\mapsto\bar{F}$*.* $\blacksquare$

The above lemma is a paraphrase of [**Roj99c**, Definition 2.3 and Main Theorem 2.3]. Furthermore, the deterministic arithmetic complexity of finding such an F^* is dominated by $\mathcal{O}(M_F\log n+n^2)$ [**Roj00d**], and can thus be ignored in our main bounds.

Lemma 6. *Following the notation above, let* $S\subset\mathbb{C}$ *be any finite set of cardinality* $\geq mV_F+1$*. Then there is an* $(\varepsilon_1,\ldots,\varepsilon_n)\in S^n$ *such that every irreducible component of* $Z_{\tilde{F}}$ *is either an irreducible component of* Z_F *or a point.* $\blacksquare$

The proof is essentially the same as the first theorem of [**GH93**, Sec. 3.4.1], save that we use part (0) of theorem 5 in place of Bézout's Theorem.

6.1.4. *The Proof of Theorem 6.*

Since we only care about the size of x_i, we can simply pick $u_0\!=\!-1$, $u_i=1$, all other $u_j\!=\!0$, and apply the polynomial h_F from theorem 5. (In particular, differing from the proof of theorem 5, we need not worry if our choice of $(u_1,\ldots,u_n)$ results in two distinct $\zeta\!\in\!Z_F$ giving the same value for $\zeta_1u_1+\cdots+\zeta_nu_n$.) Thus, by following almost the same proof as assertion (3) of theorem 5, we can beat the height bound from theorem 5 by a summand of $\mathcal{O}(n^2V_F\log D)$. $\blacksquare$

Remark 10. *Via theorem 23 (and a classic root size estimate of Cauchy* [**Mig92**]*), we easily see that the asymptotic bound for* $|\log|x_i||$ *can be replaced by explicit quantities slightly better than those stated in remark 9. In particular, it is clear from our last proof that we can simply replace the terms of the form* $\sqrt{n}\left(\binom{V_F}{2}+1\right)^n$ *in the formulae from remark 9 by* $\sqrt{2}$*.* $\blacksquare$

6.1.5. *The Proof of Theorem 7.*

All portions, save assertion (8), follow immediately from [**Roj99c**, Main Theorem 2.1]. To prove assertion (8), we will briefly review the computation of $h_1,\ldots,h_n$ (which was already detailed at greater length in [**Roj99c**]). Our height bound will then follow from some elementary polynomial and linear algebra bounds.

In particular, recall the following algorithm for computing $h_1, \ldots, h_n$, given h as in theorem 5:

Step 2 If $n = 1$, set $h_1(\theta) := \theta$ and stop. Otherwise, for all $i \in [n]$, let $q_i^-(t)$ be the square-free part of $\mathrm{Pert}_A(t, u_1, \ldots, u_{i-1}, u_i - 1, u_{i+1}, \ldots, u_n)$.

Step 3 Define $q_i^\star(t)$ to be the square-free part of $\mathrm{Pert}_A(t, u_1, \ldots, u_{i-1}, u_i + 1, u_{i+1}, \ldots, u_n)$ for all $i \in [n]$.

Step 4 For all $i \in [n]$ and $j \in \{0, 1\}$, let $r_{i,j}(\theta)$ be the reduction of $\mathcal{R}_j(q_i^-(t), q_i^\star((\alpha + 1)\theta - \alpha t))$ modulo $h(\theta)$.

Step 5 For all $i \in [n]$, define $g_i(\theta)$ to be the reduction of $-\theta - \frac{r_{i,1}(\theta)}{r_{i,0}(\theta)}$ modulo $h(\theta)$. Then define a_i to be the least positive integer so that $h_i(t) := a_i g_i \in \mathbb{Z}[t]$.

Following the notation of the algorithm above, the polynomial $\mathcal{R}_0(f, g) + \mathcal{R}_1(f, g)t$ is known as the **first subresultant** of f and g and can be computed as follows: Letting $f(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{d_1} t^{d_1}$ and $g(t) = \beta_0 + \beta_1 t + \cdots + \beta_{d_2} t^{d_2}$, consider the following $(d_1 + d_2 - 2) \times (d_1 + d_2 - 1)$ matrix

$$\begin{bmatrix}
\beta_0 & \cdots & \beta_{d_2} & 0 & \cdots & 0 & 0 \\
0 & \beta_0 & \cdots & \beta_{d_2} & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & \beta_0 & \cdots & \beta_{d_2} & 0 \\
0 & 0 & \cdots & 0 & \beta_0 & \cdots & \beta_{d_2} \\
\alpha_0 & \cdots & \alpha_{d_1} & 0 & \cdots & 0 & 0 \\
0 & \alpha_0 & \cdots & \alpha_{d_1} & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_{d_1} & 0 \\
0 & 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_{d_1}
\end{bmatrix}$$

with $d_1 - 1$ "β rows" and $d_2 - 1$ "α rows." Let M_1^1 (resp. M_0^1) be the submatrix obtained by deleting the last (resp. second to last) column. We then define $\mathcal{R}_i(f, g) := \det(M_i^1)$ for $i \in \{0, 1\}$.

Continuing our proof of Theorem 7, we see that we need only bound the coefficient growth of the intermediate steps of our preceding algorithm. Thanks to theorem 23, this is straightforward: First note that $\sigma(q_i^-) = \log((V_F + 1) \cdot 2^{V_F}) + \sigma(\bar{h}_F)$, where $\bar{h}_F$ is the square-free part of h_F. (This follows trivially from expressing the coefficients of a univariate polynomial $f(t + 1)$ in terms of the coefficients of $f(t)$.) Via lemma 4 we then see that $\sigma(\bar{h}_F) = \log(\sqrt{V_F + 1} \cdot 2^{V_F}) + \sigma(h_F)$, and thus $\sigma(q_i^-) = \mathcal{O}(\sigma(h_F))$. Similarly, $\sigma(q_i^\star) = \mathcal{O}(\sigma(h_F))$ as well.

To bound the coefficient growth when we compute $r_{i,j}$ note that the coefficient of t_i in $q_i^\star(2\theta - t)$ is exactly $(-1)^i \sum_{j=i}^{d} \begin{pmatrix} j \\ i \end{pmatrix} (2\theta)^j \alpha_j$, where α_j is the coefficient of t^j in $q_i^\star(t)$. Thus, via Hadamard's lemma again, we see that

$$|r_{i,j}(\theta)| \leq \left(\sqrt{V_F + 1} \cdot e^{\sigma(h_F)}\right)^{V_F - 1} \left(\sqrt{V_F + 1} \cdot V_F 2^{V_F} (2\theta)^{V_F} e^{\sigma(h_F)}\right)^{V_F - 1}$$

for all i, j. Since $r_{i,j}$ is itself a polynomial in θ of degree $V_F(V_F - 1)$, the last inequality then easily implies that $\sigma(r_{i,j}) = \mathcal{O}(V_F \sigma(h_F))$.

To conclude, note that for any univariate polynomials $f, g \in \mathbb{Z}[t]$ with degree $\leq D$, $\sigma(fg) = \mathcal{O}(\sigma(f) + \sigma(g) + \log D)$. Via long division it also easily follows that the quotient q and remainder r of f/g satisfy $aq, ar \in \mathbb{Z}[t]$ and $\sigma(aq), \sigma(ar) = \mathcal{O}(D(\sigma(f) + \sigma(g)))$, for some positive integer a with $\log a = \mathcal{O}(\sigma(g))$.

So by assertion (3) of theorem 5 we obtain $\log(a_i), \sigma(h_i) = \mathcal{O}(V_F^2 \sigma(h_F))$. ■

Remark 11. *An immediately consequence of our proof is that the asymptotic bound from assertion (8) can be replaced by the following explicit bound:*

$$V_F\left\{(V_F-1)\left[\log\left(V_F(V_F+1)^4 64^{V_F}\right)+2\sigma(h_F)\right]+\sigma(h_F)\right\}+\sigma(h_F)+\log V_F. \ \blacksquare$$

6.1.6. *The Proof of Theorem 4.*

Proof of Part (a): We first recall the following useful effective arithmetic Nullstellensatz of Krick, Pardo, and Sombra.

Theorem 24. *Suppose $f_1,\ldots,f_m\in\mathbb{Z}[x_1,\ldots,x_n]$ and $f_1=\cdots=f_m=0$ has* **no** *roots in $\mathbb{C}^n$. Then there exist polynomials $g_1,\ldots,g_m\in\mathbb{Z}[x_1,\ldots,x_n]$ and a positive integer a such that $g_1f_1+\cdots+g_mf_m=a$. Furthermore,*

$$\log a\leq 2(n+1)^3DV_F[\sigma(F)+\log m+2^{2n+4}D\log(D+1)]. \ \blacksquare$$

The above theorem is a portion of corollary 3 from [**KPS00**].

The proof of part (a) is then almost trivial: By assumption, theorem 24 tells us that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z}\Longrightarrow p$ divides a. Since the number of divisors of an integer a is no more than $1+\log a$ (since any prime power other than 2 is bounded below by e), we arrive at our desired asymptotic bound on a_F. $\blacksquare$

Remark 12. *Following the notation of theorem 4, we thus obtain the following explicit bound:*

$$a_F\leq 1+2(n+1)^3DV_F[\sigma(F)+\log m+2^{2n+4}D\log(D+1)]. \ \blacksquare$$

Proof of Part (b): Recall the following version of the discriminant.

Definition 4. *Given any polynomial $f(x_1)=\alpha_0+\alpha_1x_1+\cdots+\alpha_Dx_1^D\in\mathbb{Z}[x_1]$ with all $|\alpha_i|$ bounded above by some integer c, define the* **discriminant of f**, $\boldsymbol{\Delta_f}$, *to be $\frac{(-1)^{D(D-1)/2}}{\alpha_D}$ times the following $(2D-1)\times(2D-1)$ determinant:*

$$\det\begin{bmatrix}
\alpha_0 & \cdots & \alpha_D & 0 & \cdots & 0 & 0\\
0 & \alpha_0 & \cdots & \alpha_D & 0 & \cdots & 0\\
\vdots & \ddots & \ddots & & \ddots & \ddots & \vdots\\
0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_D & 0\\
0 & 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_D\\
\alpha_1 & \cdots & D\alpha_D & 0 & \cdots & 0 & 0\\
0 & \alpha_1 & \cdots & D\alpha_D & 0 & \cdots & 0\\
\vdots & \ddots & \ddots & & \ddots & \ddots & \vdots\\
0 & \cdots & 0 & \alpha_1 & \cdots & D\alpha_D & 0\\
0 & 0 & \cdots & 0 & \alpha_1 & \cdots & D\alpha_D
\end{bmatrix},$$

where the first $D-1$ (resp. last D) rows correspond to the coefficients of f (resp. the derivative of f). $\blacksquare$

Our proof of part (b) begins with the following observation.

Theorem 25. *Following the notation of section 4, suppose $f\in\mathbb{Z}[x_1]$ is a square-free polynomial of degree D with exactly i_f factors over $\mathbb{Q}[x_1]$. Then the truth of GRH implies that*

$$|i_f\pi(t)-N_f(t)|<2\sqrt{t}(D\log t+\log|\Delta_f|)+D\log|\Delta_f|,$$

for all $t>2$. $\blacksquare$

A slightly less explicit version of the above theorem appeared in [**Koi96**, Thm. 9], and the proof is almost the same as that of an earlier result of Adleman and Odlyzko for the case $i_f = 1$ [**AO83**, Lemma 3]. (See also [**Wei84**].) The only new ingredient is an explicit version of the effective Chebotarev density theorem due to Oesterlé [**Oes79**]. (Earlier versions of theorem 25 did not state the asymptotic constants explicitly.)

The proof of part (b) is then essentially a chain of elementary analytic bounds which flows from applying theorem 25 to the polynomial h_F from theorem 2. However, a technicality which must be considered is that h_F might not be square-free (i.e., Δ_{h_F} may vanish). This is easily taken care of by an application of the following immediate corollary of lemmata 3 and 4.

Corollary 2. *Following the notation above, let g be the square-free part of f and let D' be the degree of g. Then* $\log|\Delta_g| \leq D'(D\log 2 + \log(D'+1) + \log c)$. ■

Another technical lemma we will need regards the existence of primes interleaving a simple sequence.

Lemma 7. *The number of primes in the open interval* $(At^3, A(t+1)^3)$ *is at least* $\lfloor \frac{1}{12} \cdot \frac{At^2}{\log t + \log A} \rfloor$, *provided* $A, t > e^5 \approx 148.413$. ■

This lemma follows routinely (albeit a bit tediously) from theorem 8.8.4 of [**BS96**], which states that for all $t > 5$, the $t^{\underline{\text{th}}}$ prime lies in the open interval $(t\log t, t(\log t + \log\log t))$.

The key to proving theorem 4 is then to find small constants t_0 and A_F such that $N_F(A_F(t+1)^3 - 1) - N_F(A_F t^3) > 1$ for all $t \geq t_0$.

Via theorems 5 and 7, and a consideration of the primes dividing the a_i (the denominators in our rational univariate representation of Z_F), it immediately follows that $|N_F(t) - N_{h_F}(t)| \leq V_F \sum_{i=1}^{n}(\log a_i + 1)$, for all $t > 0$. We are now ready to derive an inequality whose truth will imply $N_F(A_F(t+1)^3 - 1) - N_F(A_F t^3) > 1$: By theorem 25, lemma 7, the triangle inequality, and some elementary estimates on $\log t$, t^3, and their derivatives, it suffices to require that $A_F t^2$ strictly exceed $12(\log A_F + \log t)$ times the following quantity:

$$2(1+\sqrt{2})\sqrt{3A_F t^3}[V_F(\log(3A_F t^3) + 1) + \log|\Delta_g|] + V_F\left(\log|\Delta_g| + \sum_{i=1}^{n}\log a_i + n\right) + 1,$$

for all $t > \max\{t_0, e^5\}$, where g denotes the square-free part of h_F. (Note that we also used the fact that $i_g \geq 1$.)

A routine but tedious estimation then shows that we can actually take $t_0 = 1296(\frac{1+\log 3}{3} + \log 1296) \approx 4963040.506$, and A_F as in the statement of part (b). Careful accounting of the estimates then easily yields the explicit upper bound for A_F we state below. ■

Remark 13. *The constant* $1296(\frac{1+\log 3}{3} + \log 1296)$ *arises from trying to find the least t for which $t^2 \geq \alpha \log^4 t$, where, roughly speaking, α ranges over the constants listed in the expressions for A_F, B_F, C_F, D_F below.*

$$A_F \leq \lceil 1296 B_F^2 \log^4 B_F + 36 C_F^2 \log^2 C_F + 2D_F \log D_F \rceil,$$

where

$$B_F := 72\sqrt{3}(1+\sqrt{2})V_F, \; C_F := 24\sqrt{3}(1+\sqrt{2})\log|\Delta_g| + 2, \quad \textit{and}$$

$$D_F := 12V_F\left(\log|\Delta_g| + \sum_{i=1}^{n}\log a_i + n\right) + 13. \ \blacksquare$$

6.2. Proofs of Our Results Over $\mathbb{Z}$: Theorems 17, 18, and 20.

The proof of theorems 17 and 18 rely on a refined version of Siegel's theorem (theorem 21 stated earlier in section 5) and an algorithmic result on factoring polynomials over $\mathbb{C}$ (lemma 8 below). The proof of theorem 20 will mainly use the tools we developed for our results over $\mathbb{C}$ from section 2, and is a streamlined version of the proof from [**Roj00a**].

6.2.1. *The Proof of Theorem 17.*

($\Longrightarrow$): Simply apply whatever algorithm one has for $\mathrm{Big}_{\mathbb{N}}$ to the polynomial $f(-x,-y)f(-x,y)f(x,-y)f(x,y)$ to obtain the value of $\mathrm{Big}_{\mathbb{Z}}(f)$. $\blacksquare$

($\Longleftarrow$): First calculate $b := \mathrm{Big}_{\mathbb{Z}}(f)$. If $b < \infty$ then we can simply enumerate **positive** integral points until we at last know $\mathrm{Big}_{\mathbb{N}}(f)$. (This can of course be mind-bogglingly slow, but is nevertheless a Turing-machine algorithm which is guaranteed to terminate.)

If $b = \infty$ then let us do the following: Replace f by its square-free part. (This can be done within **NC** via, say, lemma 8 below.) Then note that any irreducible component of Z_f containing infinitely many integral points must be defined over $\mathbb{Z}$. (Otherwise, the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ would imply that every integral point has multiplicity >1 — a contradiction, since the number of singular points of a curve is always finite.) So we may also assume that Z_f is geometrically irreducible. (Indeed, we can find all the irreducible components of Z_f within **NC** via lemma 8.)

Theorem 22 then tells us that $\mathrm{Big}_{\mathbb{N}}(f) = \infty \Longleftrightarrow Z_f$ has unbounded intersection with the the (open) first quadrant. To decide the latter question, one first finds the largest real critical value of the projection $(x,y) \mapsto x+y$, restricted to the intersection of Z_f with the first quadrant. (Since we are restricting to the first quadrant, one must also consider the image of the intersection of Z_f with the coordinate axes under this projection as well.) This reduces to finding the (ζ_1,ζ_2) which maximizes $\zeta_1+\zeta_2$, where (ζ_1,ζ_2) is either a positive real roots of the polynomial system $(f, \frac{\partial f}{\partial x} + \frac{\partial f}{\partial y})$, or a point in $Z_f \cap \{xy=0\}$. Thanks to theorems 5 and 7, and a fast root approximation algorithm from [**NR96**], this can be done within **NC**.

To conclude, if there is no critical value, we simply check (via the techniques just mentioned) if the polynomial system $(f, x+y-1)$ has a positive real root. It is then easily checked that this system has a root iff Z_f has unbounded intersection with the first quadrant. Otherwise, one performs the same check with the polynomial system $(f, x+y-\zeta_1-\zeta_2-1)$ instead. So we are done. $\blacksquare$

6.2.2. *The Proof of Theorem 18.*

First note that as in our last proof, we can use lemma 8 to reduce (within **NC**, relative to the dense encoding) to the case where Z_f is geometrically irreducible.

Our algorithm then proceeds as follows: Compute the genus of Z_f. (By [**KS97**], this can actually be done within **NC** as well.) If the genus is positive then theorem 21 tells us that there are only finitely many integral points and we are done. Similarly, via [**NR96**], condition (c) of theorem 21 can be checked within **NC**.

So we may now assume that Z_f satisfies condition (c) and has genus zero. Find all **positive** integral singular points of Z_f. (By theorems 5, 7, and 11, this can also be done within **NC**.) Call these points $\{(\alpha_1,\beta_1),\ldots,(\alpha_N,\beta_N)\}$. Then form the polynomial $g(x,y,t) := (x-\alpha_1)^2 + (y-\beta_1)^2 + \cdots + (x-\alpha_N)^2 + (y-\beta_N)^2 - t$. Clearly, Z_f has a nonsingular integral point iff the curve $Z_{(f,g)} \subset \mathbb{C}^3$ has a positive integral point. Furthermore, since Z_f has a rational parametrization, the curve $Z_{(f,g)}$ admits one as well. Thus $Z_{(f,g)}$ is irreducible and has genus zero too.

So assuming RatCurve(3) is decidable, theorem 21 tells us that we can decide whether Z_f has infinitely many integral points. Converting this to the decidability of $\mathrm{HTP}^\infty(2)$ is a simple matter, thanks to theorem 22 and an application of theorem 7 already detailed in our last proof. ■

Lemma 8. [**BCGW92**] *Suppose $f \in \mathbb{Q}[x_1, \ldots, x_n]$ and n is a constant. Then, relative to the dense encoding, we can find all factors of f over $\mathbb{C}[x_1, \ldots, x_n]$ within* **NC**. *Furthermore, every factor is given as a polynomial in $\mathbb{Q}[\alpha][x_1, \ldots, x_n]$, where the minimal polynomial of α is also part of the output.* ■

6.2.3. *The Proof of Theorem 20.*
It suffices to show that the truth of both conditions implies the existence of an algorithm for $\exists\exists\forall\exists$ (with all quantifiers ranging over $\mathbb{N}$), thus contradicting the aforementioned result of Matiyasevich and Robinson.

So assuming the truth of (1) and (2), let us construct such an algorithm. First note the following fact.

Lemma 9. *Following the notation above, let*

$$\Sigma_f := \{(u_0, v_0) \in \mathbb{C}^2 \ | \ \{(x,y) \in \mathbb{C}^2 \ | \ f(u_0, v_0, x, y) = 0\} \ \textit{ has a genus zero component}\}.$$

Also let Ξ_f denote the set of $(u_0, v_0) \in \mathbb{N}^2$ such that $\forall x \ \exists y \ f(u_0, v_0, x, y) = 0$. Then $\Xi_f \subseteq \Sigma_f \cap \mathbb{Z}^2$, whether all quantifiers range over $\mathbb{N}$ or $\mathbb{Z}$.

Proof of the Lemma: By theorem 21, $\forall x \ \exists y \ f(u_0, v_0, x, y) = 0 \Longrightarrow Z_f \cap \{(u,v) = (u_0, v_0)\}$ contains a curve of genus zero (whether the quantification is over $\mathbb{N}$ or $\mathbb{Z}$). So we are done. ■

Continuing the proof of theorem 20, consider the following algorithm for $\exists\exists\forall\exists$: First decide whether Z_f contains a specially ruled surface. (That this is Turing-decidable was already observed in [**Roj00a**].) If so, simply apply any algorithm for statement (2) to decide the prefix $\exists\exists\forall\exists$.

Otherwise, Σ_f is the (possibly empty) union of a finite point set and a collection of curves of positive genus. Via algorithms already observed in [**Roj00a**], the defining polynomials for all these points and curves are Turing-computable. So via theorem 7, and statement (1), the worst we need do is enumerate integral points on several curves of positive genus. So although our algorithm may be very slow, we have succeeded in deriving a contradiction, and we are done. ■

Remark 14. *The usual definition of genericity in computational algebra is stronger than the one we gave earlier: A statement involving a set of parameters $\{c_1, \ldots, c_N\}$ holds* **generically** *iff the statement is true for all $(c_1, \ldots, c_N) \in \mathbb{C}^N$ outside of some* **a priori fixed** *algebraic hypersurface. That this version of genericity implies the simplified version mentioned earlier in our theorems is immediate from Schwartz' Lemma* [**Sch80**]. *Any statement claimed to be true generically in this paper still holds under this stronger notion.* ■

7. Acknowledgements

The author would like to express his deep gratitude to the organizers of this conference for their generous invitation. The author also thanks Felipe Cucker, Ioannis Emiris, Teresa Krick, Francois Loeser, Gregorio Malajovich, Luis-Miguel

Pardo-Vasallo, Steve Smale, and Martin Sombra for some very useful discussions, in person and via e-mail. Many of the results presented in this paper would have been weaker, were it not for the wonderful atmosphere of the Hilbert 10 conference in Gent.

I dedicate this paper to Steve Smale.

Appendix: How the Examples Were Computed

Here we reveal some further details on the computations underlying our examples. All of the computations in this paper were performed on a Sun 4u Computeserver, named Kronecker, at MIT. The version of `Maple` used was `Maple V Release 5`.

The univariate reduction, $P(u)$, for our first 3×3 polynomial system is a nonzero constant multiple of the sparse resultant of f_1, f_2, f_3, and $u-xyz$. The following `Maple` code is how the computation was performed:

```
with(linalg);

f:=144+2*x-3*y^2+x^7*y^8*z^9;
g:=-51+5*x^2-27*z+x^9*y^7*z^8;
h:=7-6*x+8*x^8*y^9*z^7-12*x^8*y^8*z^7;
k:=u-x*y*z;

r1:=factor(resultant(f,k,x)):
r2:=factor(resultant(g,k,x)):
r3:=factor(resultant(h,k,x)):

rr1:=op(4,r1):
rr2:=op(4,r2):
rr3:=op(3,r3):

s1:=factor(resultant(rr1,rr3,z)):
s2:=factor(resultant(rr2,rr3,z)):

ss1:=op(4,s1):
ss2:=op(3,s2):

t:=factor(resultant(ss1,ss2,y)):
univar:=op(3,t);
```

We also note that our choice for $P(u)$ was a bit sneaky: instead of finding a polynomial whose roots were linear projection of the roots of F, we found a polynomial whose roots were a **monomial map** of the roots of F. This additional flexibility is useful in practice, and it is also possible to improve our quantitative results along these lines. These improvements will be detailed in later work, and we also point out that other applications of such nonlinear projections have appeared in earlier work of the author [**Roj98**].

As for the mixed volume calculation, we used a `C` implementation by Ioannis Emiris (publically available at
`http://www.inria.fr/saga/logiciels/emiris/soft_geo.html`). That the mixed

volume equals the number of roots in $\mathbb{C}^3$ follows easily from the fact that all the polynomials have a nonzero constant term, and an exactness condition for Bernshtein's Theorem (see, e.g., [**Ber75**] or [**Roj99a**, Main Theorem 2]). Verifying the latter condition amounts to checking whether a product of toric resultants vanishes and for the sake of brevity we omit this calculation. In any case, it is easily checked that $M_F \leq e^{3+\frac{1}{8}} \cdot \frac{243}{\sqrt{4}} + (3\cdot 9+2)^3 - (3\cdot 9+1)^3 \approx 5202.327253$ for our example, via lemma 1. (In practice, the true value of M_F is typically **much** smaller than the upper bound from lemma 1.)

By a stroke of luck, the polynomial P is irreducible over $\mathbb{Q}$, so we immediately obtain that F has exactly 145 **distinct** complex roots. Furthermore, we obtain that for any subfield $K \subseteq \mathbb{C}$, every root of P in K is the image of a unique root of F in K^3. So we also obtain that F has no rational roots. Via the `realroot` command of `Maple` (which employs **Sturm sequences** [**Roy96**]), we similarly obtain the number of real roots of F.

As for the comparison with Gröbner bases, we simply invoked the following `Maple` commands:

```
f:=144+2*x-3*y^2+x^7*y^8*z^9;
g:=-51+5*x^2-27*z+x^9*y^7*z^8;
h:=7-6*x+8*x^8*y^9*z^7-12*x^8*y^8*z^7;
k:=u-x*y*z;

with(Groebner);
univpoly(u,[f,g,h,k]);
```

The larger time bound given was actually the amount of time `Maple` spent calculating a univariate reduction via Gröbner bases, until the author's remote connection to `Kronecker` was terminated.

References

[AM75] Adleman, Leonard and Manders, Kenneth, *"NP-Complete Decision Problems for Quadratic Polynomials,"* Eighth Annual ACM Symposium on Theory of Computing (Hershey, PA, 1976), pp. 23–29, Assoc. Comput. Mach., New York, 1976.

[AO83] Adleman, Leonard and Odlyzko, Andrew, *"Irreducibility Testing and Factorization of Polynomials,"* Mathematics of Computation, 41 (164), pp. 699–709, 1983.

[BM88] Babai, L. and Moran, S., *"Arthur-Merlin Games: A Randomized Proof System and a Hierarchy of Complexity Classes,"* Journal of Computer and System Sciences, 36:254–276, 1988.

[BF91] Babai, L. and Fortnow, F., *"Arithmetization: a New Method in Structural Complexity Theory,"* Comput. Complexity **1** (1991), no. 1, 41–66.

[BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

[BCGW92] Bajaj, Chanderjit; Canny, John F.; Garrity, Thomas; Warren, Joe, *"Factoring Rational Polynomials Over the Complex Numbers,"* SIAM J. Computing 22 (1993), no. 2, pp. 318–331.

[Bak68] Baker, Alan, *"Contributions to the Theory of Diophantine Equations I: On the Representation of Integers by Binary Forms,"* Philos. Trans. Roy. Soc. London Ser. A, 263 (1968), 173–208.

[Bak69] __________, *"Bounds for the Solutions of the Hyperelliptic Equation,"* Proc. Camb. Philos. Soc. 65 (1969), 439–444.

[Bak75] __________, *Transcendental Number Theory,* Cambridge University Press, 1975.

[BC70] Baker, Alan and Coates, John, *"Integer Points on Curves of Genus 1,"* Proc. Camb. Philos. Soc. 67 (1970), 595–602.

[BGHM97] Bank, Bernd; Giusti, Marc; Heintz, Joos; Mbakop, G. M., *"Polar Varieties, Real Equation Solving, and Data Structures: the Hypersurface Case,"* J. Complexity 13 (1997), no. 1, pp. 5–27.

[Bar56] Barna, Bela, *"Über die Divergenzpunkte des Newtonschen Verfahrens zur Bestimmung von Wurzeln Algebraischer Gleichungen,"* Publ. Math. Debrecen, vol. 4, pp. 384–397 (1956).

[Bas96] Basu, Saugata, *"On Bounding the Betti Numbers and Computing the Euler Characteristic of Semi-Algebraic Sets,"* Proceedings of the Twenty-eighth Annual ACM STOC (Philadelphia, PA, 1996), pp. 408–417, ACM, New York.

[BPR96] Basu, Saugata; Pollack, Richard; Roy, Marie-Françoise, *"On the Combinatorial and Algebraic Complexity of Quantifier Elimination,"* J. ACM 43 (1996), no. 6, pp. 1002–1045.

[BLR91] Benedetti, R., Loeser, F., Risler, J. J., *"Bounding the Number of Connected Components of a Real Algebraic Set,"* Discrete and Computational Geometry, 6:191–209 (1991).

[Ber75] Bernshtein, D. N., *"The Number of Roots of a System of Equations,"* Functional Analysis and its Applications (translated from Russian), Vol. 9, No. 2, (1975), pp. 183–185.

[BP94] Bini, Dario and Pan, Victor Y., *Polynomial and Matrix Computations, Volume 1: Fundamental Algorithms,* Progress in Theoretical Computer Science, Birkhäuser, 1994.

[Bli21] Blichfeldt, H. F., *"Note on Geometry of Numbers,"* Bull. Amer. Math. Soc. **27**, pp. 150–153.

[BSS89] Blum, Lenore; Shub, Mike; Smale, Steve, *"On a Theory of Computation and Complexity Over the Real Numbers: NP-completeness, Recursive Functions and Universal Machines,"* Bull. Amer. Math. Soc. **21** (1989), no. 1, pp. 1–46.

[BCSS98] Blum, L., Cucker, F., Shub, M., Smale, S., *Complexity and Real Computation,* Springer-Verlag, 1998.

[BT99] Bogomolov, F. A. and Tschinkel, Yu., *"On the Density of Rational Points on Elliptic Fibrations,"* J. Reine Angew. Math. 511 (1999), pp. 87–93.

[Bom90] Bombieri, Enrico, *"The Mordell Conjecture Revisited,"* Ann. Sculoa Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, pp. 615–640.

[Bri84] Brindza, B., *"On S-Integral Solutions of the Equation $y^m = f(x)$,"* Acta. Math. Hungar. **44** (1984), no. 1–2, pp. 133–139.

[BCS97] Bürgisser, Peter; Clausen, Mike; and Shokrollahi, M. Amin, *Algebraic Complexity,* Grundlehren der Mathematischen Wissenschaften, 315, Springer-Verlag, 1997.

[Bür00] Bürgisser, Peter, *"Cook's Versus Valiant's Hypothesis,"* Theoretical Computer Science, special issue in honor of Manuel Blum's 60th birthday, vol. 235, no. 1, March, 2000, pp. 71–88.

[BZ88] Burago, Yu. D. and Zalgaller, V. A., *Geometric Inequalities,* Grundlehren der mathematischen Wissenschaften 285, Springer-Verlag (1988).

[Can87] Canny, John F., *"The Complexity of Robot Motion Planning Problems,"* ACM Doctoral Dissertation Award Series, ACM Press (1987).

[Can88] ______________, *"Some Algebraic and Geometric Computations in PSPACE,"* Proc. 20th ACM Symp. Theory of Computing, Chicago (1988), ACM Press.

[Can93] ______________, *"Improved Algorithms for Sign Determination and Existential Quantifier Elimination,"* Comput. J. **36** (1993), no. 5, pp. 409–418.

[CG84] Chistov, A. L., and Grigoriev, Dima Yu, *"Complexity of Quantifier Elimination in the Theory of Algebraically Closed Fields,"* Lect. Notes Comp. Sci. 176, Springer-Verlag (1984).

[Coh81] Cohen, S. D., *"The Distribution of Galois Groups and Hilbert's Irreducibility Theorem,"* Proc. London Math. Soc. (3) 43 (1981), no. 2, pp. 227–250.

[DL79] Dobkin, David and Lipton, Richard, *"On the Complexity of Computations Under Varying Sets of Primitives,"* J. of Computer and System Sciences 18, pp. 86–91, 1979.

[EC93] Emiris, Ioannis Z. and Canny, John, *"Efficient Incremental Algorithms for the Sparse Resultant and Mixed Volume,"* J. Symbolic Comput. 20 (1995), no. 2, pp. 117–149.

[Emi94] Emiris, Ioannis Z., *"Sparse Elimination and Applications in Kinematics,"* Ph.D. dissertation, Computer Science Division, U. C. Berkeley (December, 1994), available on-line at `http://www.inria.fr/saga/emiris`.

[EM99] Emiris, Ioannis Z. and Mourrain, Bernard, *"Matrices in Elimination Theory,"* J. of Symbolic Computation, 28(1&2):3-44, 1999.

[EP99] Emiris, Ioannis Z. and Pan, Victor, *"Techniques for Exploiting Structure in Matrix Formulae of the Sparse Resultant,"* Toeplitz matrices: structures, algorithms and applications (Cortona, 1996), Calcolo 33 (1996), no. 3-4, 353–369 (1998).

[Fal84] Faltings, Gerd, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern (Finiteness theorems for abelian varieties over number fields)," Invent. Math. 73 (1983), no. 3, pp. 349–366.

[FGM90] Fitchas, N., Galligo, A., and Morgenstern, J., *"Precise Sequential and Parallel Complexity Bounds for Quantifier Elimination Over Algebraically Closed Fields,"* Journal of Pure and Applied Algebra, 67:1–14, 1990.

[Gal73] Gallagher, P. X., *"The Large Sieve and Probabilistic Galois Theory,"* Analytic Number Theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis, Mo., 1972), 91–101, Amer. Math. Soc., Providence, R.I., 1973.

[Gal80] ______________, *"Some Consequences of the Riemann Hypothesis,"* Acta. Arith. 37 (1980), pp. 339–343.

[GH99] Gatermann, Karin and Huber, Birk, *"A Family of Sparse Polynomial Systems Arising in Chemical Reaction Systems,"* Preprint ZIB (Konrad-Zuse-Zentrum für Informationstechnik Berlin) SC-99 27, 1999.

[GKZ94] Gel'fand, I. M., Kapranov, M. M., and Zelevinsky, A. V., *Discriminants, Resultants and Multidimensional Determinants,* Birkhäuser, Boston, 1994.

[GH93] Giusti, Marc and Heintz, Joos, *"La détermination des points isolés et la dimension d'une variété algébrique peut se faire en temps polynomial,"* Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991), Sympos. Math. XXXIV, pp. 216–256, Cambridge University Press, 1993.

[GLS99] Giusti, M., Lecerf, G., and Salvy, B., *"A Gröbner-Free Alternative to Polynomial System Solving,"* preprint, TERA, 1999.

[Gra94] Grant, David, *"Integer Points on Curves of Genus Two and Their Jacobians,"* Trans. Amer. Math. Soc. **344** (1994), no. 1, pp. 79–100.

[GW93] Gritzmann, Peter and Wills, J., *"Lattice Points,"* in Handbook for Convex Geometry (edited by P. Gruber and J. Wills), vol. B, North Holland, Amsterdam, 1993.

[GK94] Gritzmann, Peter and Klee, Victor, *"On the Complexity of Some Basic Problems in Computational Convexity II: Volume and Mixed Volumes,"* Polytopes: Abstract, Convex, and Computational (Scarborough, ON, 1993), pp. 373–466, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 440, Kluwer Acad. Publ., Dordrecht, 1994.

[GS00] Gurvits, Leonid and Samorodnitsky, Alex, "A Deterministic Polynomial-Time Algorithm for Approximating Mixed Discriminant and Mixed Volume," Proceedings of STOC 2000, ACM Press, 2000.

[HW79] Hardy, G. H. and Wright, E. M., *An Introduction to the Theory of Numbers,* Fifth Edition, The Clarendon Press, Oxford University Press, New York, 1979.

[Har77] Hartshorne, Robin, *Algebraic Geometry,* Graduate Texts in Mathematics, No. 52, Springer-Verlag.

[HS82] Heintz, Joos and Schnorr, Claus P., *"Testing Polynomials Which are Easy to Compute,"* Logic and Algorithmic (Zurich, 1980), pp. 237–254, Monograph. Enseign. Math., 30, Univ. Genève, Geneva, 1982.

[Hir94] Hirsch, Morris, *Differential Topology,* corrected reprint of the 1976 original, Graduate Texts in Mathematics, 33, Springer-Verlag, New York, 1994.

[Ier89] Ierardi, Doug, *"Quantifier Elimination in the Theory of an Algebraically-Closed Field,"* Proc. 21st ACM Symp. Theory of Computing, Seattle (1989), 138–147.

[Jon81] Jones, James P., *"Classification of Quantifier Prefixes Over Diophantine Equations,"* Zeitschr. f. math. Logik und Grundlagen d. Math., Bd. 27, 403–410 (1981).

[Jon82] ______________, *"Universal Diophantine Equation,"* Journal of Symbolic Logic, 47 (3), 403–410 (1982).

[KLS97] Kannan, R., Lovasz, L, and Simonovitz, M., *"Random Walks and an $\mathcal{O}^*(n^5)$ Volume Algorithm for Convex Bodies,"* Random Structures Algorithms, **11** (1997), no. 1, pp. 1–50.

[Kho78] Khovanskii, A. G., *"Newton Polyhedra and the Genus of Complete Intersections,"* Functional Analysis (translated from Russian), Vol. 12, No. 1, January–March (1978), 51–61.

[Kho91] Khovanski, Askold, *Fewnomials,* AMS Press, Providence, Rhode Island, 1991.

[Koi96] Koiran, Pascal, *"Hilbert's Nullstellensatz is in the Polynomial Hierarchy,"* DIMACS Technical Report 96-27, July 1996. (**Note:** This preprint considerably improves the published version which appeared in Journal of Complexity in 1996.)

[Koi97] ____________, *"Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties,"* Proceedings of the 38th Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Oct. 20–22, 1997, ACM Press.

[KS97] Kozen, Dexter and Stefánsson, Kjartan, *"Computing the Newtonian Graph,"* J. Symbolic Comput. **24** (1997), no. 2, pp. 125–136.

[KP96] Krick, Teresa and Pardo, Luis-Miguel, *"A Computational Method for Diophantine Approximation,"* Algorithms in Algebraic Geometry and Applications (Santander, 1994), pp. 193–253, Progr. Math., 143, Birkhäuser, Basel, 1996.

[KPS00] Krick, T., Pardo, L.-M., and Sombra, M., *"Sharp Arithmetic Nullstellensatz,"* submitted for publication, also downloadable from `http://xxx.lanl.gov/abs/math.AG/9911094`.

[LO77] Lagarias, Jeff and Odlyzko, Andrew, *"Effective Versions of the Chebotarev Density Theorem,"* Algebraic Number Fields: L-functions and Galois Properties (Proc. Sympos. Univ. Durham, Durham, 1975), 409–464, Academic Press, London, 1977.

[Lan97] Lang, Serge, *Survey of Diophantine Geometry,* Springer-Verlag, 1997.

[Lec00] Lecerf, Grégoire, *"Computing an Equidimensional Decomposition of an Algebraic Variety by Means of Geometric Resolutions,"* submitted to the proceedings of the International Symposium on Symbolic Algebra and Computation (ISSAC) 2000.

[LLL82] Lenstra, A. K., Lenstra, H. W., and Lovász, L., *"Factoring Polynomials with Rational Coefficients,"* Math. Ann. 261 (1982), no. 4, 515–534.

[Len98] Lenstra, Hendrik W., *"Finding Small Degree Factors of Lacunary Polynomials,"* Number Theory in Progress, proceedings of a meeting in honor of the 70th birthday of Andrej Schnizel, W. de Gruyter, to appear.

[Mai00] Maillot, Vincent, *"Géométrie D'Arakelov Des Variétés Toriques et Fibrés en Droites Intégrables,"* Mém. Soc. Math. France, to appear.

[Mal00a] Malajovich, Gregorio, *"Condition Number Bounds for Problems with Integer Coefficients,"* Journal of Complexity, to appear september 2000.

[Mal00b] ________________, *"Transfer Theorems for the* $\mathbf{P} \neq \mathbf{NP}$ *Conjecture,"* Journal of Complexity, to appear.

[Man95] Manin, Yu. I., "Problems on Rational Points and Rational Curves on Algebraic Varieties," Surveys in Differential Geometry, Vol. II (Cambridge, MA, 1993), pp. 214–245, Internat. Press, Cambridge, MA, 1995.

[Mat73] Matiyasevich, Yuri V., *"On Recursive Unsolvability of Hilbert's Tenth Problem,"* Logic, Methodology and Philosophy of Science, IV (Proc. Fourth Internat. Congr., Bucharest, 1971), pp. 89–110, Studies in Logic and Foundations of Math., Vol. 74, North-Holland, Amsterdam, 1973.

[MR74] Matiyasevich, Yuri V. and Robinson, Julia *"Two Universal 3-Quantifier Representations of Recursively Enumerable Sets,"* Teoriya Algorifmov i Matematicheskaya Logika (Volume dedicated to A. A. Markov), 112–123, Vychislitel'nyĭ Tsentr, Akademiya Nauk SSSR, Moscow (Russian).

[Mat93] Matiyasevich, Yuri V., *Hilbert's Tenth Problem,* MIT Press (1993).

[MM82] Mayr, E. and Meyer, A., *"The Complexity of the Word Problem for Commutative Semigroups and Polynomial Ideals,"* Adv. Math. **46**, 305–329, 1982.

[MM95] McKelvey, Richard D., and McLennan, Andrew, *"The Maximal Number of Regular Totally Mixed Nash Equilibria,"* preprint, Department of Economics, University of Minnesota, 1995.

[Mig92] Mignotte, Maurice, *Mathematics for Computer Algebra,* translated from the French by Catherine Mignotte, Springer-Verlag, New York, 1992.

[Mil76] Miller, Gary L., *"Riemann's Hypothesis and Tests for Primality,"* J. Comput. System Sci. **13** (1976), no. 3, 300–317.

[Mil64] Milnor, John *"On the Betti Numbers of Real Varieties,"* Proceedings of the Amer. Math. Soc. 15, pp. 275–280, 1964.

[Mir95] Miranda, Rick, *Algebraic Curves and Riemann Surfaces,* Graduate Studies in Mathematics, Vol. 5, American Mathematical Society.

[Mor97] Morais, J. E., *"Resolucion Eficaz de Sistemas de Ecuaciones Polinomiales (Efficient Solution of Systems of Polynomial Equations),"* Ph.D. Thesis, Univ. Cantabria, Santander, 1997.

[MP98] Mourrain, Bernard and Pan, Victor, *"Asymptotic Acceleration of Solving Multivariate Polynomial Systems of Equations,"* Proc. STOC '98, pp. 488–496, ACM Press, 1998.

[Mum95] Mumford, David, *Algebraic Geometry I: Complex Projective Varieties,* Reprint of the 1976 edition, Classics in Mathematics, Springer-Verlag, Berlin, 1995.

[Mun84] Munkres, James R., *Elements of Algebraic Topology,* Addison-Wesley, 1984.

[NR96] Neff, C. Andrew and Reif, John, *"An Efficient Algorithm for the Complex Roots Problem,"* Journal of Complexity **12** (1996), no. 2, 81–115.

[Oes79] Oesterlé, Joseph, *"Versions Effectives du Théorème de Chebotarev sous l'Hypothèse de Riemann Généralisée,"* Astérisque **61** (1979), pp. 165–167.

[OP49] Oleinik, O. and Petrovski, I., *"On the Topology of Real Algebraic Hypersurfaces,"* Izv. Akad. Akad. Nauk SSSR 13, pp. 389–402, 1949.

[Pac99] Pacelli, Patricia L., *"Some Uniformity Results Following from the Lang Conjectures,"* Number Theory (Ottawa, ON, 1996), pp. 291–296, CRM Proc. Lecture Notes, 19, Amer. Math. Soc., Providence, RI, 1999.

[Pap95] Papadimitriou, Christos H., *Computational Complexity,* Addison-Wesley, 1995.

[Pla84] Plaisted, David A., *"New NP-Hard and NP-Complete Polynomial and Integer Divisibility Problems,"* Theoret. Comput. Sci. 31 (1984), no. 1–2, 125–138.

[Poo96] Poonen, Bjorn, *"Computational Aspects of Curves of Genus at Least* 2*,"* Algorithmic Number Theory (Talence, 1996), pp. 283–306, Lecture Notes in Comput. Sci., 1122, Springer, Berlin, 1996.

[Pou93] Poulakis, Dimitrios, *"Integer Points on Curves of Genus 0,"* Colloq. Math. **66** (1993), no. 1, pp. 1–7.

[Pra75] Pratt, Vaughan R., *"Every Prime has a Succinct Certificate,"* SIAM J. Comput. **4** (1975), 327–340.

[Ren92] Renegar, Jim, *" On the Computational Complexity and Geometry of the First-Order Theory of the Reals, I–III,"* J. Symbolic Comput. 13 (1992), no. 3, pp. 255–352

[Roj98] Rojas, J. Maurice, *"Intrinsice Near Quadratic Complexity Bounds for Real Multivariate Root Counting,"* Proceedings of the Sixth European Symposium on Algorithms (ESA '98, Venice), Lecture Notes in Computer Science 1461, pp. 127–138, 1998.

[Roj99a] ________________, *"Toric Intersection Theory for Affine Root Counting,"* Journal of Pure and Applied Algebra, vol. 136, no. 1, March, 1999, pp. 67–100.

[Roj99b] ________________, *"On the Complexity of Diophantine Geometry in Low Dimensions,"* Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC '99, May 1–4, 1999, Atlanta, Georgia), pp. 527–536, ACM Press, 1999.

[Roj99c] ________________, *"Solving Degenerate Sparse Polynomial Systems Faster,"* Journal of Symbolic Computation, vol. 28 (special issue on elimination theory), no. 1/2, July and August 1999, pp. 155–186.

[Roj00a] ________________, *"Uncomputably Large Integral Points on Algebraic Plane Curves?,"* Theoretical Computer Science, special issue in honor of Manuel Blum's 60th birthday, vol. 235, no. 1, March, 2000, pp. 145–162.

[Roj00b] ________________, *"Some Speed-Ups and Speed Limits for Real Algebraic Geometry,"* Journal of Complexity, FoCM 1999 special issue, to appear.

[Roj00c] ________________, *"Computational Arithmetic Geometry I: Sentences Nearly in the Polynomial Hierarchy,"* J. Comput. System Sci., STOC '99 special issue, to appear.

[Roj00d] ________________, *"The Geometry of Elimination I: Complexity and Height Bounds,"* Journal of Symbolic Computation, special issue on recent progress on resultants, to appear.

[RY00] Rojas, J. Maurice and Ye, Yinyu, *"Solving Fewnomials in Near Logarithmic Time,"* submitted for publication.

[Roy96] Roy, Marie-Françoise, *"Basic Algorithms in Real Algebraic Geometry and their Complexity: from Sturm's Theorem to the Existential Theory of Reals,"* Lectures in Real Geometry (Madrid, 1994), pp. 1–67, de Gruyter Exp. Math., 23, de Gruyter, Berlin, 1996.

[Rud76] Rudin, Walter, *Principles of Mathematical Analysis,* 3rd edition, McGraw-Hill, 1976.

[Sch82] Schinzel, Andrzej, *Selected Topics on Polynomials,* Univ. of Michigan Press, Ann Arbor, 1982.

[Sch92] Schmidt, Wolfgang M., *"Integer Points on Curves of Genus 1,"* Compositio Mathematica **81**: 33–59, 1992.

[Sch80] Schwartz, J., *"Fast Probabilistic Algorithms for Verification of Polynomial Identities,"* J. of the ACM 27, 701–717, 1980.

[Sha94] Shafarevich, Igor R., *Basic Algebraic Geometry I,* second edition, Springer-Verlag (1994).

[Shu93] Shub, Mike, *"Some Remarks on Bézout's Theorem and Complexity Theory,"* From Topology to Computation: Proceedings of the Smalefest (Berkeley, 1990), pp. 443–455, Springer-Verlag, 1993.

[Sie29] Siegel, Carl Ludwig, *"Über einige Anwendungen Diophantischer Approximationen,"* Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), Nr. 1.

[Sil95a] Silverman, Joseph H., *"Counting Integer and Rational Points on Varieties,"* Columbia University Number Theory Seminar (New York, 1992), Astrisque No. 228, (1995), 4, pp. 223–236.

[Sil95b] ________________, *The Arithmetic of Elliptic Curves,* corrected reprint of the 1986 original, Graduate Texts in Mathematics 106, Springer-Verlag (1995).

[Sil00] ________________, *"On the Distribution of Integer Points on Curves of Genus Zero,"* Theoretical Computer Science, special issue in honor of Manuel Blum's 60th birthday, vol. 235, no. 1, March, 2000, pp. 163–170.

[Sma98] Smale, Steve, *"Mathematical Problems for the Next Century,"* Mathematical Intelligencer, to appear (1998).

[SY82] Steele, J. and Yao, A., *"Lower Bounds for Algebraic Decision Trees,"* J. of Algorithms 3, pp. 1–8, 1982.

[Sto85] Stockmeyer, Larry, *"On Approximation Algorithms for $\#\mathbf{P}$,"* SIAM Journal on Computing, 14(4):849–861, 1985.

[Stu94] Sturmfels, Bernd, *"On the Newton Polytope of the Resultant,"* Journal of Algebraic Combinatorics, 3: 207–236, 1994.

[Stu98] ______________, *"Introduction to Resultants,"* Applications of Computational Algebraic Geometry (San Diego, CA, 1997), 25–39, Proc. Sympos. Appl. Math., 53, Amer. Math. Soc., Providence, RI, 1998.

[Sun92] Sun, Zhi Wei, *"A New Relation-Combining Theorem and its Application,"* Z. Math. Logik Grundlag. Math. 38 (1992), no. 3, pp. 209–212.

[Tho65] Thom, René, *"Sur l'homologie des variétés algébriques réelles,"* In S. Cairns (Ed.), Differential and Combinatorial Topology, Princeton University Press, 1965.

[Tun87] Tung, Shih-Ping, *"Computational Complexities of Diophantine Equations with Parameters,"* Journal of Algorithms **8**, 324–336 (1987).

[Tun99] ______________, *"Sentences Over Integral Domains and their Computational Complexities,"* Inform. and Comput. 149 (1999), no. 2, pp. 99–133.

[Van50] van der Waerden, B. L., *Modern Algebra,* 2nd edition, F. Ungar, New York, 1950.[36]

[Voj87] Vojta, Paul, *Diophantine Approximations and Value Distribution Theory,* Lecture Notes in Mathematics, 1239, Springer-Verlag (1987).

[WZ94] Weiman, Jerzy and Zelevinsky, Andrei, *"Multigraded Formulae for Multigraded Resultants,"* J. Algebraic Geom. 3 (1994), no. 4, pp. 569–597.

[Wei84] Weinberger, Peter, *"Finding the Number of Factors of a Polynomial,"* Journal of Algorithms, 5:180–186, 1984.

[Zac86] Zachos, S., *"Probabilistic Quantifiers, Adversaries, and Complexity Classes: An Overview,"* Proc. 1st Structure in Complexity Theory Conference, vol. 223, Lecture Notes in Computer Science, Springer-Verlag, 1986.

Department of Mathematics, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, HONG KONG

E-mail address: mamrojas@math.cityu.edu.hk, *Web-Page:* http://www.cityu.edu.hk/ma/staff/rojas

[36] Shamefully, the sections on resultants were removed from later editions of this book.